Opinnäytetyö (AMK)

Tietojenkäsittely

Yrityksen tietoliikenne ja tietoturva

2016

Sanna Lehtonen

LUOTTAMUKSELLISEN TIEDON SÄILYTTÄMINEN

– salaisen tiedon luokittelu sekä henkilöstökoulutus yrityksessä

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Yrityksen tietoliikenne ja tietoturva

2016 | 58

Sanna Lehtonen

LUOTTAMUKSELLISEN TIEDON SÄILYTTÄMINEN

- salaisen tiedon luokittelu sekä henkilöstökoulutus yrityksessä

Tiedon luokittelussa pyritään tunnistamaan ja merkitsemään yrityksen tieto sen suojaustoimenpiteiden mukaisesti. Prosessi on tärkeä osa yrityksen tiedon turvaamista, sillä määritellyn luokan perusteella voidaan ottaa käyttöön oikeat suojaustoimet. Tiedon luokittelu ja salaisen tiedon käsittely olivat osa kohdeyrityksellä käynnissä olevaa tietosuojaprojektia, ja se toteutetaan kohdeyrityksen lisäksi myös muualla Pohjoismaissa.

Tämän opinnäytetyön tarkoituksena oli tutustua yrityksen tiedon luokitteluun ja eritoten luottamuksellisen eli salaisen tiedon käsittelyyn ja säilytykseen. Yritykseen implementoitiin salaiselle tiedolle varattu säilytyspaikka, josta järjestettiin henkilöstökoulutuksia asianomaisille henkilöille. Tavoitteena oli tutustua erilaisiin tiedon säilytysmahdollisuuksiin sekä maailmalla yleisiin luokittelupolitiikkoihin, ja verrata näitä yritykselle käyttöön tulevaan politiikkaan ja tiedon säilytyspaikkaan.

Opinnäytetyön teoreettisessa viitekehyksessä tutustuttiin yleisiin tiedon luokittelun menetelmiin ja luottamuksellisen tiedon määritelmään sekä luokitteluun. Tiedon luokittelun pohjana käytettiin ISO/IES 27001 -standardia, joka määrittelee tiedon luokituksen yrityksessä. Luottamuksellisen tiedon luokittelun keskeisiä osa-alueita tutkittiin yleisiin menetelmiin tutustumalla. Osa-alueisiin voidaan laskea kuuluviksi tiedon paikantaminen, luokittelu ja suojaaminen. Tutkimuksen kohteena olivat myös erilaiset tiedon säilytysmenetelmät ja mahdollisuudet pilvipalveluiden hyödyntämiseen luottamuksellisen tiedon säilyttämisessä. Säilytysmenetelmiksi voidaan tässä tapauksessa laskea muun muassa jaetut verkkolevyt, SharePointiin perustuvat ratkaisut sekä pilvipalveluntarjoajan tarjoamat vaihtoehdot tiedon säilytykseen.

Empiirisessä osuudessa haastateltiin kohdeyrityksen työntekijää erään toisen yrityksen luokittelupolitiikasta. Haastattelun tuloksia käytettiin kohdeyrityksen ja haastattelussa käsitellyn yrityksen keskinäisessä vertailussa. Kohdeyrityksen tiedon luokittelupolitiikkaa tarkasteltiin ja arvioitiin käyttäjän näkökulmasta. Tarkoituksena oli selvittää kuinka selkeät ohjeistukset ja vaatimukset yrityksellä on tarjolla tiedon luokitteluun. Käyttäjille tehtiin suomennetut ohjeet konsernilla käytössä olevista tiedon luokittelun ohjeistuksista sekä tarjolla olevista työkaluista. Ohjeet julkaistaan yrityksen intranetissä. Henkilöstökoulutuksessa pyrittiin huomioimaan käyttäjät ja avartamaan heidän tietämystään salaisen tiedon luokittelusta. Lisäksi koulutuksessa esiteltiin luokittelun apuna käytettäviä työkaluja ja tietojen uutta säilytyspaikkaa. Palaute koulutuksista oli erittäin positiivista, joten lisäkoulutuksia pidetään tarvittaessa.

ASIASANAT:

tiedon luokittelu, tietoturva, luottamuksellinen tieto, tiedon säilytys.

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Business Data Communications and Information Security

2016 | 58

Sanna Lehtonen

HOW TO STORE CONFIDENTIAL INFORMATION

- information classification and implementing a staff training session in a company

Information classification means identifying and labeling company's information and applying proper protection. The process is an important part of protecting company's information. Information classification and handling secret information were part of a bigger project in the company in question. Later on it will also be implemented in other Nordic countries.

The purpose of this thesis was to familiarize oneself with a company's information classification policy and especially how to handle and store confidential and secret information. Storage for secret information has been implemented in the company so staff training sessions on this matter were held for the designated staff. The objective was to study different possibilities of storing information and how classification policies were used worldwide and then compare them with the company's policy and storage.

The theoretical part of this thesis consists of examining/studying globally used methods of classifying information and how to define and classify confidential information. Information classification is based on the ISO/IES 27001 standard which defines how to classify information in a company. The primary points of classifying confidential information were studied, such as identifying and securing information and different classifying methods. Different methods of storing information and the possibility of using cloud storages were also studied. In this case, methods of storage include File Shares and different solutions of SharePoint and cloud provider.

In the empirical part, an employee of the company was interviewed about his previous employer's information classification policy and the results were used to compare the two companies. The current company's information classification regulations were studied and the policy was analyzed from the viewpoint of a user. Translated instructions about information classification and usable tools were created for users. The goal of the staff training session was to widen the audience’s knowledge about how to classify secret information. The respective tools and the new secret information storage were also presented in the training. Feedbacks about the trainings were positive so there will be extra training if needed.

KEYWORDS:

information classification, information security, confidential information, information storage.

SISÄLTÖ

LIITTEET

TAULUKOT

KÄYTETYT LYHENTEET JA SANASTO

Ad Hoc File Transfer	Suurien tiedostojen siirtoon käytettävä työväline
BitLocker	Windowsissa käytettävä salausominaisuus (Microsoft 2016a)
BYOD	Bring Your Own Device, oman laitteen käyttäminen työskennellessä (Bradley 2016)
Connections	Yrityksen sisäinen sosiaalinen verkosto tiedon ja uutisten jakamiseen
CWID	Konsernin henkilötunniste (The Free Dictionary By Farlex 2016)
Data	Merkkejä tai symboleita sisällään pitävä tieto (Huotari 2016)
Digitaalinen allekirjoitus	Lähettäjän viestin loppuun liittämä tiiviste tekstistä (Hakala ym. 2006, 377)
DLP	Data Loss prevention, tietovuotojen ehkäisy (Woody 2013, 144)
FIPS 199	Federal Information Processing Standard 199 (Barker 2008, 7)
IEC	International Electrotechnical Commission (IEC 2016)
Informaatio	Välitettävää, siirrettävää tai viestitettävää tietoa (Huotari 2016)
ISO	Internal Organization for Standardization, kansainvälinen standardisoimisjärjestö (ISO 2016)
Kryptaus	Tiedon salaaminen eli muuttaminen muotoon, josta ainoastaan tietyt henkilöt saavat sen auki (Hakala ym. 2006, 372)
Lync	Ajantasainen viestintäsovellus (Microsoft 2016b)
Rakenteellinen tieto	Riveissä ja sarakkeissa sijaitseva tieto (EMC Education Services 2012, 6)
Rakenteeton tieto	Riveihin tai sarakkeisiin sopimaton tieto (EMC Education Services 2012, 6)
Tieto	Pitää sisällään datan, informaation, tiedon ja viisauden (Huotari 2016)
VPN	Virtual Private Network, virtuaalinen erillisverkko (Cisco 2008)

1 JOHDANTO

Tiedon luokittelussa pyritään tunnistamaan ja merkitsemään yrityksen tieto sen suojaustoimenpiteiden mukaisesti. Prosessi on tärkeä osa yrityksen tiedon turvaamista, sillä määritellyn luokan perusteella voidaan ottaa käyttöön oikeat suojatoimenpiteet. Tiedon luokittelu ei ole Suomessa kovinkaan tunnettu tiedon suojauksen ala, joten tavoitteena on tarjota mahdollisimman helppokäyttöiset ja vaatimukset täyttävät menetelmät tiedon luokitteluun ja suojaukseen. Tässä opinnäytetyössä pyritään selventämään yrityksen salaisen tiedon luokittelupolitiikan vaatimuksia henkilöstölle ohjeiden ja koulutusten avulla.

Teoriaosuudessa tutustutaan maailmalla hyväksyttyihin tiedon luokittelun menetelmiin ja luottamuksellisen tiedon luokittelussa huomioon otettaviin seikkoihin. Lisäksi tutkitaan pilvipalveluiden käytettävyyttä salaisen tiedon säilytyksessä. Empiirisessä osuudessa yrityksen tiedon luokittelun ohjeet käännetään suomeksi ja salaisen tiedon käsittelyä koskevat ohjeistukset kootaan yhdelle dokumentille. Yritykselle käyttöön tulevaan salaisen tiedon säilytyspaikkaan tutustutaan, ja tämän sekä tehtyjen ohjeiden pohjalta kootaan koulutusmateriaali. Työssä käytetään laadullisen tutkimuksen menetelmää, jossa on hankepainotteisen toimintatutkimuksen piirteitä.

Tiedon luokittelu ja salaisen tiedon käsittely ovat osa yrityksellä käynnissä olevaa tietosuojaprojektia. Tiedon luokittelu on omana alaprojektinaan ja Suomen jälkeen se toteutetaan myös muissa Pohjoismaiden toimipisteissä. Koulutusmateriaalista tehdään myös englanninkielinen versio.

Tässä opinnäytetyössä sanaa *tieto* käytetään viittaamaan yrityksen sähköisesti säilöttyä tietoa. Tämä käsittää sekä datan että informaation, jotka kummatkin kuuluvat *tietoon*.

2 TIEDON LUOKITTELU

2.1 Tiedon määritelmä

Tiedon voidaan sanoa pitävän sisällään neljä eri määritelmää: datan, informaation, tiedon ja viisauden. Data käsitetään merkkejä tai symboleita sisällään pitävänä tietona, kun taas informaatio on välitettävää, siirrettävää tai viestitettävää. Tieto (knowledge) syntyy, kun informaatio muuttaa tiedon prosessointitapaa, ja kun tällä tavoin oppimaansa käyttää hyväkseen, tarkoittaa se viisautta. (Huotari 2016.)

Tässä opinnäytetyössä käytän sanaa *tieto* viittaamaan dataan ja informaatioon ja jätän edellä määrittelemäni tiedon ja viisauden käsittelemättä, sillä kyseiset määritelmät eivät ole työssäni oleellisia.

2.2 Tiedon luokittelun määritelmä

Tiedon luokittelu on yrityksen tiedon tunnistamista, ja sen merkitsemistä kuvaamaan tiedon suojaamiseen tarvittavia toimenpiteitä riskit ja arvot huomioon ottaen (Woody 2013, 143). Eri tiedon luokittelutasot ovat tulleet alun perin armeijan käyttämistä termeistä: *unclassified, sensitive-but-unclassified, confidential, secret* ja *top secret*, jotka muokattiin yrityksen tarpeisiin sopiviksi. Tiedon luokittelun voidaan ajatella olevan suorassa vaikutuksessa yrityksen oman liiketoimintaprosessin perustason ymmärtämisessä, joten on ensiarvoisen tärkeää ottaa käyttöön mahdollisimman kuvaavat termit. (Etges & McNeil 2006.)

Tiedon luokittelu voi olla yksinkertainen kaavio tai monimutkainen ratkaisu, joka vahvistaa tiedon luokittelua sen luomishetkellä. Ensi alkuun suositellaan yksinkertaisten prosessien kehittämistä ja implementointia, minkä jälkeen näitä voidaan vahvistaa luomalla yksityiskohtaisempia ja monimutkaisempia ratkaisuja. (Woody 2013, 143.)

2.2.1 FIPS 199 -standardi

FIPS 199 eli Federal Information Processing Standard 199 määrittää turvallisuuskategoriat, objektiivit ja seuraustasot vahingon määrään perustuen. Turvallisuustavoitteisiin

kuuluvat luotettavuus, loukkaamattomuus sekä saatavuus. Luotettavuuden menetys tarkoittaa tässä tapauksessa tiedon luvatonta paljastumista, kun taas loukkaamattomuuden menetys merkitsee luvatonta tiedon muokkausta tai tuhoamista. Saatavuuden menetys on häiriötä tiedon tietojärjestelmään käsiksi pääsyssä tai käytössä. (Barker 2008, 9–10.)

Vahingon määritelmistä matala vahinko käsittää tehtävän suorittamiseen liittyvän kapasiteetin laskemisen, mikä ei kuitenkaan estä päätehtävien suorittamista aiheuttaen näin ainoastaan vähäistä vahinkoa tavoitteiden saavuttamisessa. Lievä vahinko saattaa aiheuttaa vakavia haittoja operaatioihin, hyödykkeisiin tai henkilöihin aiheuttaen merkittävää taloudellista menetystä. Tämä saattaa johtaa myös henkilövahinkoihin aiheuttamatta kuitenkaan hengenvaaraa. Korkea vahinko aiheuttaa erittäin vakavia tai jopa katastrofaalisia haittoja henkilöille ja hyödykkeille. Pahimmassa tapauksessa se saattaa johtaa hengenlähtöön ja suureen taloudelliseen vahinkoon. (Barker 2008, 9–10.)

2.2.2 ISO/IES 27001 -standardi

ISO/IES 27001 -standardi määrittää eri luokitukset yrityksen hyödykkeille ja niille sopivat turvatoimenpiteet. Standardin mukaan kaikki yrityksen toimijat jakavat vastuun tiedon suojaamisesta. Yrityksen johto tai tiedon omistajat ovat vastuussa tiedon luokittelusta ja siitä, että nämä luokitukset ohjaavat koko henkilöstön toimintaa. Kaikki yrityksessä oleva tieto voidaan jakaa neljään seuraavanlaiseen kategoriaan:

- luokittelematon julkinen tieto
- omistusoikeudellinen tieto
- asiakasluottamuksellinen tieto
- yritysluottamuksellinen tieto.

Luokittelematon julkinen tieto ei ole luottamuksellista, ja se voidaan julkistaa aiheuttamatta ongelmia yritykselle eikä tiedon saatavuuden menettäminen esimerkiksi järjestelmän kaatumisen vuoksi aiheuta suurta riskiä. Omistusoikeudellinen tieto puolestaan on rajattu ainoastaan johdon käyttöön ja suojattu ulkopuoliselta pääsyltä. Luvaton pääsy kyseisiin tietoihin saattaa vaikuttaa yrityksen toiminnalliseen tehokkuuteen, aiheuttaa taloudellista vahinkoa, tarjota merkittävää hyötyä kilpailijalle tai vahingoittaa asiakastyytyväisyyttä. Tiedon loukkaamattomuuden säilyminen on näin ollen ensiarvoisen tärkeää. (Information Classification Policy 2016.)

Asiakasluottamuksellinen tieto on kaikissa tapauksissa luottamuksellista, oli tieto missä muodossa tahansa. Alkuperäiseen tietoon ei tule kajota ilman asiakkaalta saatua kirjallista lupaa tietojen muuttamiseen. Yrityksen keräämä ja käyttämä tieto henkilöiden työllistämisestä, lokeista, asiakastilauksien täyttämisestä ja muista yrityksen näkökohdista sen liiketoiminnassa ovat yritysluottamuksellista tietoa ja näin ollen vaativat korkeimman mahdollisen loukkaamattomuuden, luottamuksellisuuden ja rajatun saatavuuden tason. Kyseiset vaatimukset pätevät myös asiakasluottamukselliseen tietoon. (Information Classification Policy 2016.)

2.3 Tiedon luokitteluperiaatteet

Tiedon luokittelu on aloitettava korkeatasoisella liiketoiminnan vaikutusten analyysillä, jonka avulla tunnistetaan kriittinen liiketieto. Analyysin tulosten perusteella kyetään selvittämään kaksi tärkeintä palaa tiedon jäljittämisessä: tietojärjestelmät ja infrastruktuuriosat, joista määritellään ne osat jotka ovat kriittistä tietoa. (Etges & McNeil 2006.)

Tiedon luokittelussa on huomioitava seuraavat seikat:

- Tiedon luokittelun merkityksen ja vaatimusten selvittäminen
- Yritykselle tärkeän tiedon tunnistaminen
- Toimeenpantujen toimien monitoroitavuus ja paranneltavuus
- Henkilöstökoulutuksen järjestäminen
- Ympäristön suojaamisen lisäksi, itse tiedon suojaaminen
- IT-osaston ja talouspuolen yhteistyöongelmien ehkäisy. (Simberkoff 2016.)

Edellä mainittujen seikkojen lisäksi yrityksen on pidettävä mielessä, ettei kaikkea jo olemassa olevaa tietoa suositella erikseen luokiteltavaksi. Mikäli tiedon luokittelussa käytetään ulkoistettua menetelmää, saattaa lopputulos tulla yllättävän kalliiksi. (Mohamed 2008.) Yrityksellä itsellään on selkein mielikuva tiedon suojauksen tarpeesta ja siitä, mitkä tiedot on suojattava. Ulkoisen toimijan tuotos saattaa näin ollen olla ainoastaan ohjeistus, eikä aina sovi yrityksen tarpeisiin. Samasta syystä myös riskianalyysi ja tiedon luokittelu on syytä pitää erillään. Riskianalyysissä arvo määritetään mahdollisten rahallisten menetysten kautta. Tieto ei itsessään tuota mitään, joten tällainen tuottoihin perustuva määrittely hankaloittaa tiedon arvon määrittelyä. (Fowler 2003, 1–5.)

Mikäli riskianalyysiä halutaan käyttää hyväksi myös tiedon luokittelun kohdalla, on syytä arvioida riskien seurauksia myös muihin kuin rahallisiin menetyksiin perustuen. Tiedon arvon määrittelyssä onkin pyrittävä aina ottamaan huomioon tiedon luonne. Esimerkiksi henkilötietojen katsotaan kuuluvan yksityisyydensuojan piiriin. Niiden vuotaminen ulkopuolisten tietoon ei välttämättä aiheuta yritykselle taloudellista haittaa, mutta todennäköisesti vahingoittaa yrityksen mainetta joko työntekijöiden tai asiakkaiden silmissä.

Tiedon luokittelu ei ole hintasidonnaista, antaen näin yrityksille paljon joustavuutta ja mahdollistaen ainoastaan tärkeisiin asioihin keskittymisen. Lisäksi tietoturvan ja tiedon periaatteet määrittelemällä työntekijöille annetaan selkeät tavoitteet. Kattava lähestymistapa tekee tiedon luokittelusta haastavampaa, joten moni yritys pyrkii tavoitteissaan tiedon saatavuuden ja oikeellisuuden varmistamiseen. (Fowler 2003, 1–5.)

2.4 Tiedon suojaaminen

Eri yrityksillä on erilaiset lähestymistavat tiedon suojaamiseksi, mutta tavoitteena lähes kaikilla on pyrkimys tarkentaa yrityksen turvatoimia arvot ja riskit huomioiden. Yrityksen antama virallinen lausunto tiedon suojaamisen tarpeesta on ensimmäinen askel tavoitteiden saavuttamisessa. Virallinen tietolähteiden dokumentointi ja vastuuhenkilöiden ylös kirjaaminen varmistaa loukkaamattomuuden ja luottamuksellisuuden toteutumisen tarjoamalla puitteet sille, että oikeat ihmiset työskentelevät oikean asian parissa. Järjestelmien saatavuuden varmistamisessa resurssien tehokkuus on avainasemassa suurten hintaerojen vuoksi. Tärkeimpinä päättävinä elementteinä voidaan pitää järjestelmän palautumisnopeutta mahdollisen toimintahäiriön koittaessa ja tiedon priorisointia yritykselle tärkeimpien tietojen palauttamiseksi. (Fowler 2003, 1–5.)

Varmuuskopioinnin merkitys on suuressa asemassa tiedon palauttamisessa. Tietoa tallennetaan suuret määrät tietokoneen kiintolevyille sekä jaettaville verkkoasemille. Jos luottamuksellista tai oikeusasiallista tietoa tallennetaan ja säilytetään verkkolevyillä, on näistä säännöllisesti otettava varmuuskopiot. Suuret kiinto- ja verkkolevytilat aiheuttavat nykypäivänä sen ettei vanhentuneiden tietojen poistamisesta huolehdita riittävän tehokkaasti. Varmuuskopiot saattavat tarpeellisten tietojen lisäksi sisältää paljon turhaa tietoa tai useita kopioita samasta dokumentista. Tässä tapauksessa jonkinlaisen tiedon analysointityökalun implementoiminen saattaa tulla tarpeeseen. (Järvinen 2006, 324, 338.)

Käyttöoikeuksia määrittämällä voidaan tehokkaasti rajata tietoihin pääsy ainoastaan ennalta määrätyille henkilöille. Oikeudet määritellään usein henkilön tunnuksille, joiden avulla tämä kirjautuu yrityksen tietokoneelle. Yleensä yrityksen työntekijälle annetaan ensin ainoastaan perusoikeudet, joita lähdetään laajentamaan sitä mukaan kun tarve vaatii. Käyttäjät jaetaan usein kolmeen ryhmään, joihin kuuluvat käyttäjäryhmät (users), järjestelmänvalvojat (administrators) ja tehokäyttäjät (power users). Käyttäjäryhmillä on oikeudet ainoastaan sovellusten käyttämiseen työasemalla, kun taas järjestelmänvalvojilla on täydet oikeudet ja tehokäyttäjillä lähestulkoon täydet. (Hakala ym. 2006, 124–126).

Tiedon suojausta ei kuitenkaan tule jättää ainoastaan oikeuksien rajoittamisen varaan, vaan on muistettava myös koulutuksien tärkeys. Kouluttamaton henkilöstö voi tahattomasti aiheuttaa yritykselle suuria vahinkoja paljastamalla tietoja huijareille. Fyysisten laitteiden ja tiedon itsensä ollessa turvattu, on tarpeen investoida käyttäjien kouluttamiseen tiedon käsittelyn ja suojaamisen suhteen. Yritykset ovat jatkuvasti huijausten kohteena, ja social engineeringiksi kutsuttu tietojen kalastelu on yleistynyt vuosi vuodelta (Woody 2013, 188). Käyttäjien ollessa tietoisia vaaroista ja käsittelemänsä tiedon tärkeydestä, vähentyy tietomurtojen ja -vuotojen riski huomattavasti.

3 LUOTTAMUKSELLINEN TIETO JA SEN LUOKITTELU

Tiedon luokitteluprosessin alussa tieto on tunnistettava ja rajattava sen mukaan mitä tietoa yritys tarvitsee toimiakseen. Tiedon tunnistamisen jälkeen on selvitettävä missä tieto sijaitsee ja näiden perusteella luodaan yksityiskohtainen tiedon luokittelumalli, jota käytetään pohjana tiedon käsittelyn säädöksille. Näin ollen tiedon luokittelumallin on oltava helposti ymmärrettävissä, jotta tiedon tunnistaminen on mahdollisimman yksinkertaista. Yrityksellä saattaa olla useita toiminnalle tärkeitä tietotyyppejä, joihin voi kuulua patentoitua tai tavaramerkittyä omaisuutta, säädeltyä tietoa tai muita tunnistamisen vaativia kategorioita. Kaikilla yrityksillä on hallussaan tietoa, joka on jollain tavalla suojattava. (Woody 2013, 138–139.)

Tyypillisiin tietotyyppeihin kuuluvat:

- henkilöstötiedot
- yrityksen yksityinen tieto
- yrityksen luottamuksellinen tieto
- yrityksen julkinen tieto
- asiakastiedot
- lääketieteellinen tieto. (Woody 2013, 138–139.)

3.1 Luottamuksellisen tiedon paikantaminen

Tietoa saattaa sijaita useissa eri paikoissa kuten työnantajan sekä työntekijän omistamissa laitteissa tai sisäisissä ja ulkoisissa verkoissa (Woody 2013,139). Aiemmin tiedon tuli sijaita ainoastaan yrityksen omistamissa laitteissa, mutta Bring Your Own Device (BYOD) ajattelutavan myötä tieto voi sijaita lähes missä vain. BYOD-termillä tarkoitetaan työntekijän käyttävän henkilökohtaista laitettaan yrityksen tietojen käsittelyssä. Monet yritykset tukevat kyseistä ajattelutapaa siitä saatavien kulusäästöjen vuoksi, mutta tämä aiheuttaa myös tietoturvariskejä tiedon siirtyessä pois yrityksen ympäristöstä. (Bradley 2016.)

Monet työntekijät lähettävät työhön liittyviä sähköposteja omaan henkilökohtaiseen sähköpostiinsa aikomuksenaan työskennellä kotona. Työntekijä pyrkii olemaan tehokas,

mutta aiheuttaakin toimillaan sen että yrityksen tietoa sijaitsee ohjelmissa ja sovelluksissa, jotka eivät ole yrityksen hallinnan alla. Kyseisissä sijainneissa suojaukset eivät välttämättä ole samaa tasoa kuin yrityksen ympäristössä, mikä altistaa tiedon tietosuojariskeille. (Woody 2013, 139.)

Tässä tapauksessa VPN-yhteyden implementoiminen yritykseen saattaa ratkaista ongelman. Remote-Access VPN tai VPDN (Virtual Private Dial-up Network) mahdollistaa suojatun pääsyn yrityksen verkkoon. VPN-yhteyttä käyttämällä yrityksen työntekijä kykenee työskentelemään kotonaan suojatun yhteyden avulla. Tämä vähentää tarvetta lähettää työasioita omaan henkilökohtaiseen sähköpostiosoitteeseen ja ehkäisee näin myös tietovuotojen syntymistä. (Cisco 2008.)

Tiedon sijainnin määrittäminen saattaa olla erittäin manuaalinen prosessi ilman tiedon löytämiseen kehitettyjen työkalujen käyttöä. Kyseisten työkalujen avulla voidaan määrittää tietyt kriteerit, joihin yrityksen tietoa verrataan. Tätä metodia voidaan kuitenkin käyttää ainoastaan yrityksen omaisuuteen, joten BYOD-käytännön omaksuneet yritykset joutuvat käyttämään muita menetelmiä yksityisyydensuojan rikkomisen välttämiseksi. Tästä syystä yrityksen saattaa olla viisainta kieltää luottamuksellisen tiedon käsittely työntekijän omistamalla laitteella. Toinen vaihtoehto on käyttää suojattuja virtuaalisia isäntäkoneita, jotka mahdollistavat yrityksen laitteiden kanssa työskentelyn tarkkaan kontrolloidussa ympäristössä. (Woody 2013, 141–142.)

3.2 Luottamuksellisen tiedon luokittelu

Kun kaikki tieto on luokiteltu, voidaan luoda yksinkertainen taulukko eri tietotyypeistä ja niiden luokittelusta sekä turvatoimista (Taulukko 1). Taulukon tulisi toimia pohjana tiedon luokittelussa ja suojaamisessa. (Woody 2013, 143.)

Alla on esimerkki taulukosta, jossa on määritelty tiedon tyyppi eri luokkatasojen mukaan. Taulukko perustuu kohdeyrityksen tiedon luokittelupolitiikkaan ja eri tietotyyppien esimerkit on esitetty taulukossa erittäin yleisellä tasolla. *Secret*-luokkaan kuuluu salainen tieto, johon voidaan laskea kuuluvaksi muun muassa tutkimustulokset sekä keksintöilmoitukset. Näiden suojatoimenpiteisiin kuuluu tiedon salaus ja pääsyn rajoittaminen. *Restricted*-tietoon voidaan laskea kuuluvaksi esimerkiksi luottamuksellisten projektien dokumentoinnit ja niissä riittävänä suojauksena pidetään oikeuksien rajausta. *Internal*-tietoon puolestaan katsotaan kuuluvaksi kaikki yrityksen julkinen tieto, johon ei ole tarpeen implementoida erillisiä suojatoimenpiteitä.

Taulukko 1. Tiedon luokittelumalli.

	Secret	**Restricted**	**Internal**
Tiedon tyyppi	Tutkimustulokset, keksintöilmoitukset	Projektien dokumentointi, laskut	Intranetuutiset, henkilöstölehdet, yleiset ohjeet
Suojatoimenpiteet	Tiedon salaus, rajattu pääsy	Rajattu pääsy	Ei suojatoimenpiteitä

Hyväksytty luokittelumalli on otettava koko yrityksen käyttöön. Tiedon omistajien on hyvä olla viimeisimpien tiedon suojaustoimien tarkistusten kohteena, ja suositeltavaa on, että IT-osasto on myös mukana opastamassa. Varsinainen vastuu tiedon suojaamisesta on kuitenkin koko yrityksen henkilöstöllä. Tyypillisesti tiedon luokittelu epäonnistuu kommunikaatio-ongelmien vuoksi. Tämän ehkäisemiseksi on suositeltavaa järjestää aika ajoin kyselyitä tiedon luokittelusta, jotta voidaan kartoittaa lisäkoulutuksen tarvetta. (Woody 2013, 143–144.)

3.3 Tiedon omistajien määrittäminen

Tiedon omistajan määrittäminen on erittäin tärkeässä asemassa onnistuneen tiedon luokittelun varmistamisessa. Omistajien nimittäminen tuo vastuullisuutta ja vähentää tiedon löytämisestä aiheutuvaa arvailua. Omistajilta on saatava selvyys prosessien sisältämästä tiedosta, jotta kyetään ymmärtämään mitä se on, kuka sitä käyttää, kuinka sitä käytetään ja minne se on sijoitettu. Näin kyetään varmistamaan oikeiden turvatoimien implementoiminen tiedon luokitteluvaiheessa. (Woody 2013, 142.)

Onnistuneen tiedon luokittelun varmistamiseksi, on tärkeää ottaa tiedon omistajat mukaan tiedon suojaamisen suunnitteluun mahdollisimman aikaisessa vaiheessa. Näin heille syntyy parempi ymmärrys tiedon turvaamiseen vaadittavista toimista vähentäen riskien syntymistä. Tieto siitä mitä muut tiimit tekevät omistajan tiedolla lisää yhteistyöhalukkuutta ja vähentää IT:n turvallisuusvalvonnan tarvetta. (Woody 2013, 142.)

3.4 Luottamuksellisen tiedon suojaaminen

Yritysten tarve e-dokumenttien jakamiseen ja eri osastojen välisen yhteistyön harjoittamiseen asettaa omat haasteensa tietoturvan toteuttamiselle. Luottamuksellinen materiaali tulisi suojata mahdollistaen kuitenkin sen jakamisen. Eräänä keinona voidaan esimerkiksi käyttää Microsoft Officen tarjoamaa tiedostojen ja sähköpostiviestien salausta. Luottamuksellisia tiedostoja poistaessa on pyyhittävä puhtaaksi tiedon koko sijainti, jotta voidaan varmistaa tiedon tuhoutuvan kokonaan. Tietokoneille pääsyä voidaan myös fyysisesti rajoittaa tai ottaa tietokone kokonaan pois verkosta. Keinoja on useita, mutta monet saattavat hankaloittaa tai hidastaa työntekoa. (Smallwood & Blair 2012, 128–129.)

Salausmenetelmää käyttämällä tieto muutetaan muotoon, josta ainoastaan tietyt henkilöt saavat sen auki. Tähän tarvitaan kirjoitusavain, jota on käytetty tiedon salaamiseen ja mahdollisesti myös jokin muu menetelmä. Salauksessa voidaan käyttää muun muassa salaisen avaimen arkkitehtuuria, jossa käytetään ainoastaan yhtä avainta tiedon salaamiseen ja purkamiseen. Menetelmä on käytännöllinen siinä tapauksessa että tiedon parissa työskentelee useampi kuin yksi ihminen. Tässä on kuitenkin omat vaaransa, sillä avaimen päätyminen ulkopuolisen tietoon saattaa tuottaa suuria ongelmia. (Hakala ym. 2006, 372.)

Digitaalista allekirjoitusta käytetään viestin lähettäjän henkilöllisyyden varmistamisessa. Menetelmässä viestistä tehdään tiiviste, jonka allekirjoittaja salakirjoittaa ja liittää lähettämänsä viestin loppuun. Viestin salakirjoittamisessa käytetään allekirjoittajan salaista avainta ja se avataan tämän julkisella avaimella, joka toimitetaan vastaanottajalle. (Hakala ym. 2006, 377.)

3.5 Tietovuotojen ehkäiseminen

Data Loss Prevention (DLP) -nimitystä käytetään työkalusta, jonka avulla voidaan vahvistaa luokitellun tiedon suojausta. Tiedon sijaitessa useassa eri paikassa jonkinlainen automatisoitu prosessi sen löytämiseen on tarpeen. DLP auttaa tietojen löytämisessä eri sijainneista ja voi joissain tapauksissa myös vahvistaa kryptausta, estää turvattomia lähetyksiä ja luvattomia kopiointeja sekä arkistointeja. (Woody 2013, 144.)

Työkalu käy läpi kaikki e-dokumentit ja sähköpostiviestit ennen niiden välittämistä organisaation ulkopuolelle, noudattaen järjestelmänvalvojan määrittämiä sääntöjä. (Smallwood & Blair 2012, 138). DLP:n päätarkoitus on estää tiedon luvaton vuotaminen, joten on tärkeää selvittää kuinka se voidaan implementoida ympäristöön tuottamaan odotettuja tuloksia (Woody 2013, 144).

DLP:tä on käytetty onnistuneesti tiedonkulun kartoittamiseen yrityksen sisällä sekä siitä poistuttaessa. Tällä pystytään seuraamaan mitä reittiä tieto kulkee, jotta voidaan implementoida kehittyneempiä tiedon kartoittamiseen, tarkkailuun ja suojaamiseen olevia menetelmiä. Tästä on ollut enemmän hyötyä kuin DLP:n käyttämisestä ainoastaan tiedon turvaamisen parantamiseen. Teknologia ei ole tarpeeksi nopeaa, jotta se voisi siepata kaiken. Jos näin kuitenkin olisi, niin joukkoon mahtuisi myös paljon luottamuksellista tietoa sisältäviä viestejä, joita lähettäjillä on oikeus välittää eteenpäin. Tällaisessa tapauksessa jonkun on käytävä vapauttamassa DLP:n väärin perustein sieppaamat viestit, jotta niiden matka tiedon vastaanottajalle voi jatkua. DLP ei myöskään kykene tunnistamaan ja monitoroimaan salattuja sähköpostiviestejä, sillä se luottaa menetelmässään sisällön tutkimiseen. (Smallwood & Blair 2012, 138.)

4 LUOTTAMUKSELLISEN TIEDON SÄILYTYSMENETELMÄT

Tiedon säilytykseen suunniteltuja laitteita kutsutaan yleensä tallennuslaitteiksi (storage device) (EMC Education Service 2013, 9). Tietoa voidaan säilyttää usealla eri tavalla, joista yleisimpiä ovat jaetut verkkolevyt, tietokannat, dokumenttien säilytystilat, pilvipalveluiden tarjoamat säilytyspaikat ja ulkoiset tallennuslaitteet. Säilytyssijaintien arvioinnissa on otettava huomioon yrityksen politiikka, standardit ja tiedon luokittelumalli. (Woody 2013, 145.)

4.1 Tiedon luokittelun automatisointiin kehitettyjä työkaluja

Yrityksissä oleva tieto voidaan luokitella joko rakenteelliseksi tai rakenteettomaksi tiedoksi. Rakenteellinen tieto on organisoitu riveihin tai kolumneihin ennalta määriteltyyn muotoon. Tämä mahdollistaa sovellusten tehokkaan tiedonhaun ja -käsittelyn. Tietoa sanotaan rakenteettomaksi jos sen elementtejä ei voida sijoittaa riveihin tai kolumneihin, hankaloittaen näin sovellusten tiedon löytämistä. Rakenteettomaksi tiedoksi voidaan käsittää esimerkiksi .doc- .txt- ja .pdf-tiedostot. (EMC Education Services 2012, 6.)

SharePoint

SharePoint on Microsoftin kehittämä selainpohjainen ohjelmistoalusta, joka on suunniteltu erityisesti yritysten käyttöön. SharePoint mahdollistaa ajantasaisen yhteistyön, dokumenttien säilytyksen sekä yrityksen intranetin luomisen. SharePointin sisällön näkevät ainoastaan yrityksen työntekijät ja käyttäjien oikeuksien hallinnointia voidaan erittäin tarkasti säädellä. SharePointissa on huomioitu *eDiscovery*, joka liittyy oikeusasiallisten dokumenttien löytämiseen, sekä *Records Management*, joka tarjoaa useita ominaisuuksia tallenteiden järjestämiseen. (Withee 2013, 9–10, 19–20.)

Smarter Document Management

SDM:n eli Smarter Document Managementin avulla pyritään automatisoimaan tai puoliautomatisoimaan manuaalista tiedon lisäämistä. Kyseisen menetelmän avulla lisätään tarkkuutta ja tehokkuutta liiketoiminnassa. SDM:n avulla voidaan vähentää varkauksia ja asiakasyksityisyyden menettämistä dokumenttien sisällöt analysoimalla. (Xerox Corporation 2016.)

EMC Infoscape

EMC Infoscape löytää, luokittelee sekä hallinnoi järjestelemätöntä tietoa tiedoston koko elinkaaren ajalta sen arvoon perustuen. EMC Infoscapen avulla voidaan implementoida tiedon hallinnointipalveluita, kuten esimerkiksi säilytysaikaa ja tietoturvaa. Tiedolle voidaan määrittää säännöt, joiden perusteella EMC Infoscape löytää ja luokittelee tietoa sekä selvittää mitä toimenpiteitä vaaditaan seuraavaksi. Tiedon siirto oikeaan paikkaan on automatisoitua ja käyttäjille läpinäkyvää tarkoittaen tässä tapauksessa sitä, että käyttäjät voivat jatkaa tiedon entisen polun käyttämistä tiedon olinpaikan muuttamisen jälkeenkin. (EMC Corporation 2006, 17).

4.2 Luottamuksellisen tiedon sijoittaminen pilveen

Pilvipalvelut ovat helposti käytettäviä ja saatavia virtualisoituja resursseja, jotka ovat dynaamisesti konfiguroitavissa sekä nopeasti tarjottavissa ja vapautettavissa minimaallisilla hallintatoimenpiteillä tai palveluntarjoajan toimilla (National Institute of Standards and Technology 2016). Pilvipalveluiden potentiaali tietoturvan ja joustavuuden parantamisessa on merkittävä ja yksinkertaisesti sanottuna kaikki turvatoimet ovat halvempia suuremmalla skaalalla implementoituna. Pilvipalveluiden useat sijainnit mahdollistavat tiedon kopioinnin moneen eri paikkaan parantaen näin vikatilanteesta palautumista. Lisäksi varhaisessa vaiheessa havaittuihin tietoturvauhkiin voidaan vastata entistä tehokkaammin ja paremmin. Joissain tapauksissa voidaan myös palkata asiantuntija työskentelemään tiettyjen uhkien parissa. (ENISA 2009, 17.)

Riskit tulisi aina ajatella osana yleistä liiketoimintamahdollisuutta ja riskinottohalukkuutta. Pilvipalveluntarjoajalla on monesti erittäin suuri kontrolli tietoturvaan vaikuttavista seikoista, mikä saattaa asiakkaalla johtaa hallinnanmenetykseen. Voi olla vaikeaa tarkistaa

palveluntarjoajan tiedonkäsittelymenetelmien lainmukaisuutta. Asiakas ei näin ollen voi olla varma siitä, että tietoa käsitellään ja turvataan niin kuin kuuluu. Palveluntarjoajan vaihtaminen saattaa myös osoittautua ongelmalliseksi, sillä tiedon, sovellusten ja palveluiden siirtämiseen tarkoitettuja työkaluja on vähäinen määrä. Asiakas ei voi siirtää kaikkea vastuuta pilvipalveluntarjoajalle, sillä jos riski johtaa liiketoiminnan epäonnistumiseen tai yrityksen maineen menettämiseen, on muiden lähes mahdotonta korvata tästä aiheutunutta vahinkoa. (ENISA 2009, 9–10, 23.)

Yritykset ovat pilvipalveluiden ilmaantumisesta lähtien olleet hyvin epäluuloisia tietojen sijoittamisesta pilveen. Syynä tähän on usein se, ettei pilvipalveluista vieläkään tiedetä tarpeeksi, joten luotettavan palveluntarjoajan löytäminen saattaa olla hyvinkin haastavaa. Pilvipalveluiden käytön yleistyttyä myös yritykset pohtivat mahdollisuuksia siirtää osan tiedoista pilveen. Monissa yrityksissä joko on jo siirrytty käyttämään pilvipalveluita tai pohditaan parhaillaan kuinka niitä voisi parhaiten hyödyntää.

4.3 Esimerkkejä pilvipalveluntarjonnasta

SpiderOak

SpiderOak on yhdysvaltalainen pilvipalveluntarjoaja, joka tarjoaa tiedon säilytystilaa ja varmuuskopiointia. Yritys mainostaa itseään turvallisena säilytyspaikkana *end-to-end* salausominaisuuden ansiosta, jonka avulla tiedot salataan ennen niiden lähettämistä pilveen. Näin ainoastaan asiakkaalla säilyy avain tiedon salauksen purkamiseen, mahdollistaen sen ettei tietoja pääse avaamaan ja näkemään kukaan ulkopuolinen. Teoriassa tämä tarkoittaisi myös sitä, ettei itse palveluntarjoajakaan pääse näkemään sisältöä. SpiderOakin salaustapa ei kuitenkaan ole avointa lähdekoodia, joten ei ole pystytty varmistamaan väitteen todenperäisyyttä. Asiakkaan on siis itse päätettävä luottaako siihen, ettei yritys ole sijoittanut koodiin eräänlaista takaporttia, jonka avulla pääsee asiakkaan tietoihin käsiksi. Kirjautuminen SpiderOakiin nettisovelluksen avulla aiheuttaa jonkinasteisen turvallisuusriskin, sillä salasana on annettava palvelimelle sen varmistamista varten. Edward Snowdenin tapauksen vuoksi yrityksen sijaintikin saattaa aiheuttaa joillekin asiakkaille huolta. Monet suosivatkin yrityksiä, joiden tietokeskukset sijaitsevat muualla kuin Yhdysvalloissa. (Crawford 2015.)

Tresorit

Kuten SpiderOak myös Tresorit tarjoaa tiedon säilytystilaa sekä helppoon tiedon jakamiseen käytettäviä työkaluja. Tresorit sijaitsee Sveitsissä, joten käyttäjät hyötyvät maan vahvoista tiedon suojauksen laeista. Asiakasohjelman päässä tapahtuva salaus on käytössä myös Tresoritilla, mikä tuo luotettavuutta yrityksen toimintaan ja tietoturvaan. Tresorit käyttää suljettua lähdekoodia, joten ei voida olla täysin varmoja siitä, päätyvätkö käyttäjän salausavaimet kolmannelle osapuolelle. Yrityksen sijainnin perusteella voidaan kuitenkin olla suhteellisen varmoja siitä, ettei näin käy. Yritys tarjosi 50 000 dollarin palkinnon kenelle tahansa, joka onnistuu murtamaan sen tietoturvan vuosina 2013–2014. Kilpailu oli käynnissä 468 päivää eikä kyseisenä aikana kukaan kyennyt murtamaan yrityksen tietoturvaa ja vaatimaan palkintoa itselleen. (Crawford 2014.)

5 SALAISEN TIEDON LUOKITTELU KOHDEYRITYKSESSÄ

5.1 Salaisen tiedon säilytyspaikkojen ja sovellusten vaatimukset

Analysoin yritykselle implementoitavana olevaa *Protection Requirements for Classified Information Storage and Application Services* -dokumenttia talletuspaikkojen ja sovellusten vaatimuksista. Heti dokumentin alussa korostetaan saatavuuden, luotettavuuden ja eheyden varmistamisen tärkeyttä, minkä mainitaan olevan myös yrityksen *IT Security* -ohjeistuksessa ja näiden merkitys yritykselle selvennetään dokumentissa. Kyseiset määritelmät ovat perusvaatimuksia kaikessa tietosuojaan liittyvässä, joten niiden huomioon ottaminen on ensiarvoisen tärkeää. Luokiteltuja tietoluokkia yrityksellä on yhteensä kolme, mutta käsittelen analyysissäni ainoastaan *Secret*-tietoa koskevia vaatimuksia.

Dokumentti koostuu kahdesta taulukosta, joista toinen käsittelee yrityksen sisäisesti hallinnoitavia palveluita ja toinen ulkoisesti hallinnoitavia. Eri luokat ja niiden vaatimukset on jaoteltu selkeästi ja kattavasti. Tosin ehdotettaessa jotain ratkaisua olisi hyvä lisätä jonkinlainen esimerkki muualla käytetyistä ratkaisuista, jotta tiedetään minkä tyyppistä tapaa lähdetään etsimään. Pelkästä taulukosta ei aina myöskään käy ilmi mitä milläkin vaatimuksen kohdalla oikein tarkoitetaan.

Menetelmien on oltava ensisijaisesti mahdollisimman käyttäjäystävällisiä ja turvallisia. Tätä silmällä pitäen yrityksen IT-osastolle on annettu vastuu käyttäjätilien ja oikeuksien hallinnasta. Lisäksi ulkoisten työntekijöiden käyttäjätilien ja oikeuksien hallinnoinnin mainitseminen dokumentissa on erittäin tärkeää, sillä monessa yrityksessä kyseiset asiat jätetään helposti huomioimatta, mikä saattaa aiheuttaa vakavia aukkoja tietoturvassa. Administraattorioikeudet on myös tarkoin määritelty, ja niitä myönnetään ainoastaan tarvittaessa.

5.1.1 Salauksen merkitys

Dokumentissa korostetaan salauksen merkitystä eri tilanteissa. Tiedostojen, säilytyspaikkojen ja laitteiden salaamisella kyetään estämään ulkopuolisten pääsy käsiksi luot-

tamukselliseen materiaaliin. Salausta vaaditaan joko salaisten dokumenttien ympäristöltä tai itse tiedostoilta tarkoittaen sitä, että jos tiedon säilytysympäristöä ei ole salattu, on salattava itse salaiset tiedostot. Yksittäisten tiedostojen salaaminen saattaa aiheuttaa käyttäjille ylimääräistä vaivaa, mikäli he eivät voi käyttää Microsoft Officen tarjoamaa salausmenetelmää. Yrityksessä hyväksytty 7-zip-ohjelman käyttö on hieman monimutkaisempaa ja enemmän aikaa vievää. Tästä johtuen käyttäjillä olisi hyvä olla jo valmiiksi salattu ympäristö, jonne he voisivat tallettaa salaiset dokumenttinsa. Tällöin käyttäjän ei tarvitsisi kuluttaa aikaa tiedoston salaamiseen ja salasanojen turvalliseen tallettamiseen.

Sähköpostiviestien salaaminen onnistuu Microsoft Outlookilla, tosin ulkoiselle kumppanille viestejä lähetettäessä salaus vaatii hieman enemmän työtä. Sekä vastaanottajan että lähettäjän on ennen salausta hyväksyttävä toistensa allekirjoitukset ja kummallakin on oltava päällä tietyt asetukset sähköpostissa. Salauksen aiheuttamat haasteet on otettu huomioon yrityksessä järjestettävässä salaista tietoa koskevassa koulutuksessa ja salaamisesta on luotu ohjeet käyttäjille.

5.1.2 Tiedon luokittelu ja hallinnointi

Kaikista salaisista dokumenteista on käytävä ilmi niiden luokitus, joka voidaan merkitä Wordissa ja PowerPointissa olevalla Labeling Toolilla. Työkalu on erittäin käyttäjäystävällinen eikä hankaloita työntekoa. Suurena ongelmana voidaan kuitenkin pitää sitä, ettei Excel-tiedostoja voi luokitella työkalun avulla. Kyseiset tiedostot jäävät siis jatkossakin luokittelematta, mikä saattaa aiheuttaa sekaannusta tai tiedon käsittelijän puolelta tapahtuvia luokitteluvirheitä. Voidaan kuitenkin luottaa siihen että tiedon omistaja todennäköisesti osaa välittää tiedon luokittelusta eteenpäin ja ilmoittaa vastaanottajalle kuinka kyseistä tietoa tulisi käsitellä.

Vaatimuksissa mainitaan myös turvallisesta tiedon hävityksestä. Tiedon tuhoamisessa on käytettävä niille tarkoitettuja hävittämistapoja. Fyysisillä laitteilla on oltava omat lukitut roska-astiansa ja elektronisilla tiedoilla erikseen hyväksytyt tuhoamistavat. Lisäksi luottamukselliset tiedot on pyrittävä tuhoamaan ainoastaan yrityksen omissa tiloissa. Yrityksellä on panostettu materiaalin oikeaoppiseen ja turvalliseen hävittämiseen sijoittamalla eri materiaaleille määriteltyjä roska-astioita rakennukseen.

5.1.3 Kolmannen osapuolen palvelut

Kolmannen osapuolen tarjoamassa palvelussa turvatoimet ovat tiukemmat, mutta pääpiirteissään samat mitä yrityksen sisäisellä palvelulla. Käyttäjätilien ja oikeuksien hallinnointi on jonkin verran tarkempaa ja tunnistautumisessa vaaditaan kaksivaiheista tunnistautumista. Lisäksi salaisen tiedon säilytyspaikan on oltava erossa muista asiakkaista ja tieto on säilöttävä salattuna.

Palvelun hallinnoinnissa on huomioitava ISO 20000 ja 27001-standardit, jotka käsittävät ohjeistukset palvelunhallinnan järjestelmävaatimuksista ja tiedon luokittelun säädöksistä. Kolmannen osapuolen on noudatettava kyseisiä standardeja sekä tarjottava auditointeja yrityksen niin pyytäessä. Lisäksi ulkopuolisen kumppanin on raportoitava yritykseen liittyvistä tapahtumista ajallaan, ja administraattorien on oltava hyvin koulutettuja ja luotettavia.

5.1.4 Johtopäätökset

Dokumentissa on pyritty ottamaan huomioon kaikki tärkeimmät tietoturvaan liittyvät asiat yrityksen tiedon suojaamiseksi. Taulukosta näkee selkeästi eri tietoluokkien tarvitsemat turvatoimet mitkä IT-osastolla tulisi ottaa huomioon ja osastolle onkin annettu suurin vastuu elektronisesta tietosuojasta. Esimerkkien puutteen vuoksi dokumentti jättää paljon valinnanvapautta menetelmien toteuttamiseen, mikä saattaa toisaalta aiheuttaa väärinkäsityksiä. Esimerkkien avulla voitaisiin tarjota suosituksia yrityksen tarpeisiin sopivista ratkaisuista, joilla tietoa suojattaisiin.

5.2 Ohjeistus salaisen tiedon käsittelyyn yrityksessä

Tiedon luokittelu (Information Classification) on osa *Information Security* -projektia, jonka tavoitteena on auttaa yrityksen henkilöstöä käsittelemään yritystietoja vastuullisesti. On ensiarvoisen tärkeää tietää, kuinka salaista tietoa tulee käsitellä oikein, jotta se ei päädy vääriin käsiin. Tätä silmällä pitäen henkilöstölle on annettu keinot luokitella luomansa dokumentit Microsoft Word- ja PowerPoint-ohjelmiin sisältyvällä Labeling Tool -työkalulla.

5.2.1 Tiedon luokittelu

Tiedot on jaettu yrityksellä kolmeen luokkaan:

- **Internal**: Yrityksen koko henkilöstön tiedossa oleva tieto, jonka väärinkäyttö on erittäin epätodennäköistä ja aiheuttaisi vain vähäistä tai ei lainkaan haittaa.
- **Restricted**: Oletusluokitus kaikelle vielä luokittelemattomalle tiedolle. Tätä luokittelua käytetään myös silloin, kun tieto ei sovi *Internal*- tai *Secret*-luokitusten alle. *Restricted*-luokan tietoa pääsevät tarkastelemaan ainoastaan tietyt ryhmät, ja tällaisen tiedon paljastumisesta aiheutuva vahinko on vähäinen tai kohtalainen.
- **Secret**: Pitää sisällään kaiken yritykselle arvokkaan ja tärkeän tiedon, joka saattaa myös kiinnostaa kilpailijoita. Tietoon käsiksi pääsevien ryhmien määrä on erittäin rajattu. *Secret*-luokan tieto edustaa yritykselle merkittävää kilpailuetua tai paljastaa heikkouksia, mistä johtuen tiedon vuotaminen saattaisi aiheuttaa erittäin suurta vahinkoa yrityksen maineelle, toiminnalle tai myynnille.

Aina kun käsittelee salaisia dokumentteja, on hyvä miettiä jo etukäteen, mitä turvatoimenpiteitä on otettava huomioon tiedon salassa pysymisen takaamiseksi siltä varalta, että itse luo salaisia dokumentteja tai joutuu niitä tarkastelemaan.

5.2.2 Dokumentin elinkaari

Dokumentti käy elinkaarensa aikana läpi eri vaiheita. Se luodaan, arkistoidaan tai tallennetaan jonnekin, sitä muokataan, siirretään, tulostetaan ja lopulta hävitetään. Jokainen vaihe vaatii hieman erilaisia turvatoimia dokumentin käsittelyssä. Kun laatii uuden dokumentin, on hyvä muistaa luokitella se heti alussa Word- ja PowerPoint-ohjelmista löytyvällä Labeling Tool -työkalulla, joka luo dokumentin alatunnisteen kohdalle leiman dokumentin luokituksesta. Tämä helpottaa dokumentin vastaanottajan työtä sen luokituksen tunnistamisessa ja varotoimenpiteiden suorittamisessa.

Dokumentin tekijän on oltava helposti löydettävissä, eikä kyseistä tietoa saa poistaa tai muokata, sillä dokumentin tekijä on usein myös sen omistaja. Omistajan lupaa tarvitaan esimerkiksi, jos dokumentti lähetetään edelleen, sitä muokataan tai se tulostetaan. Tekijän voi nähdä *File*-välilehdellä oikealla sijaitsevasta kohdasta *related people*.

Salaisia dokumentteja ei saa säilöä ihan minne vain, vaan niille on määrätty omat säilytyspaikat. Kun tiedostoja tallennetaan Secure SharePointiin, on hyvä muistaa kaikkien sinne tallennettujen tiedostojen olevan salattuja niin kauan, kuin ne ovat Secure SharePointissa, mutta salaus häviää, kun ne ladataan omalle koneelle. Secure SharePointin erottaa tavallisesta SharePointista sen kulmassa olevasta punaisesta merkistä, jossa lukee *Secure Environment*, mutta muutoin sivusto näyttää samalta ja toimii samoin kuin tavallinen SharePoint. Ainoa merkittävä ero on se, ettei sitä ole turvallisuussyistä yhdistetty yrityksen sisäiseen hakuun.

Jaettuja verkkolevyjä tulee käyttää tiedon säilytykseen ainoastaan siinä tapauksessa, että *Secret*-tason tietojen määrä on rajallinen. Tämä vaihtoehto koskee siis lähinnä henkilöitä, jotka joutuvat ajoittain tarkastelemaan salaisiksi luokiteltuja dokumentteja. Verkkolevylle tallennettaessa salauksen merkitys korostuu entisestään, ja kaikki salaisiksi luokitellut dokumentit onkin salattava ennen niiden tallentamista. On kuitenkin muistettava, että salaamisen jälkeen dokumentin saa auki ainoastaan salasanan avulla. Siksi on erittäin tärkeää säilyttää salasana turvallisesti esimerkiksi KeePassin avulla. Salauksessa suositellaan käytettäväksi joko MS Officen salausta tai 7-zipiä.

Salaisia dokumentteja ei suositella säilytettäväksi tavallisella SharePoint-sivulla, omalla koneella tai ulkoisilla laitteilla. Nämä vaihtoehdot ovat ainoastaan rajalliselle määrälle salaisia dokumentteja ja dokumentit kyseisiin paikkoihin on salattava ennen tallentamista. SharePointiin tallennettaessa on ensin varmistettava sivun omistajalta, saako kyseisen dokumentin tallentaa sivustolle. Ulkoista laitetta (USB) käytettäessä on suositeltavaa salata koko laite BitLockerin avulla. Tulostettuja dokumentteja tulee käsitellä erityisen huolellisesti, eikä niitä saa jättää valvomatta. Silloin kun niiden parissa ei työskennellä, ne tulisi sijoittaa lukolliseen ympäristöön, kuten esimerkiksi lukittuun laatikostoon. Salaisia dokumentteja ei saa missään nimessä säilyttää Connectionsissa, tietokoneen työpöydällä tai Outlookissa.

Dokumenttia edelleen lähetettäessä on muistettava aina pyytää lupa sen omistajalta. Lupa voidaan myöntää yhdelle dokumentille kerrallaan, ja salaisen tiedon omistajan on myös mahdollista delegoida tehtävä jollekin läheiselle työtoverilleen. Yrityksen sisällä ja sen ulkopuoliselle työntekijälle sähköpostitse lähetettävät tiedot on aina ensin salattava ja allekirjoitettava sähköisesti. Jos tiedon välittämisessä käytetään USB-laitetta, laite on ensin salattava, ja sitä on myös muistettava käsitellä turvallisesti.

Lync-ohjelmaa voi käyttää dokumenttien lähetykseen siinä tapauksessa, että vastaanottajalla on yrityksen CWID-tunnus. Yrityksen ulkopuolisten yhteistyökumppanien kanssa on noudatettava erityistä varovaisuutta ja tiedostot on lähetettävä salattuina Ad Hoc File Transferin kanssa. Salauksen salasanaa ei saa lähettää sähköpostitse, vaan se on annettava joko puhelimitse tai tekstiviestillä. Tulostetut dokumentit toimitetaan henkilökohtaisesti tai luotettavaa lähettiä käyttäen.

Salaista dokumenttia muokatessa on huomioitava dokumentin sen hetkinen luokitus ja pidettävä se samana, ellei tiedon luonne muutu radikaalisti. Jos useampia henkilöitä työskentelee saman dokumentin parissa, on dokumentin omistajan pidettävä huoli siitä, että kaikilla kyseisillä henkilöillä on oikeudet dokumentin muokkaukseen. Edellä mainitut säännöt pätevät myös kokouksissa jaettavaan tietoon.

Tulostettuja asiakirjoja on käsiteltävä erittäin huolellisesti, ja niiden säilytystä varten olisi hyvä olla varattuna lukollinen kaappi tai laatikosto. Tulostettaessa, tulostinta ei saa jättää valvomatta sinä aikana, kun tulostustoiminto on käynnissä. Jos henkilö ei pääse itse paikalle valvomaan tulostusta, hänen on pyydettävä luotettavaa osapuolta varmistamaan, etteivät ulkopuoliset henkilöt pääse käsittelemään asiakirjoja. Tulostettaessa on pyrittävä käyttämään pull print tai secure printing -tulostusta, joihin tarvitaan käyttäjän tunnistautuminen. Asiakirjasta ei saa ottaa useita kopioita ilman omistajan lupaa, ja kotitulostimen käyttö salaisten asiakirjojen tulostukseen on ehdottomasti kielletty.

Hävitettäessä salaisia dokumentteja on käytettävä tarkoitukseen varattua roska-astiaa tai silppuria. Tiedostoja poistaessa on muistettava tyhjentää tietokoneen työpöydällä oleva Roskakori. Kaikki salaiset dokumentit on hävitettävä ainoastaan yrityksen tiloissa.

6 YKSILÖHAASTATTELU JA HENKILÖSTÖKOULUTUS

6.1 Haastattelu ulkopuolisen yrityksen tiedon luokittelupolitiikasta

Haastattelussa tavoitteena oli verrata ulkopuolisen yrityksen tiedon luokittelupolitiikkaa kohdeyrityksen lanseerattavana olevaan politiikkaan. Haastateltava oli aiemmin työskennellyt toisessa yrityksessä, josta vaihtoi kohdeyrityksen alaiseksi. Haastateltava ei siis haastattelun aikana toiminut toisen yrityksen edustajana, ja haastattelussa esitetyt mielipiteet ja näkökulmat ovat hänen omiaan.

Haastattelumetodina käytettiin teemahaastattelua, jossa keskityttiin haastateltavan aikaisemman työnantajan tiedon luokittelupolitiikkaan. Haastattelua käytettiin myöhemmin kohdeyrityksen ja toisen yrityksen keskinäisessä vertailussa. Haastattelumuotona oli yksilöhaastattelu, joka järjestettiin haastateltavan omassa työhuoneessa. Kysymykset lähetettiin haastateltavalle ennakkoon, jotta hän ehti valmistelemaan vastauksiaan varsinaista haastattelua varten. Haastateltava ei täyttänyt erillistä kyselylomaketta, vaan haastattelu suoritettiin suullisesti 4.2.2016. Haastattelun materiaali koottiin ja jäsenneltiin kokonaisuudeksi haastattelun jälkeen, ja valmis versio lähetettiin haastateltavalle tarkistettavaksi mahdollisten korjaustoimien varalta. Haastattelussa esitetyt kysymykset on korostettu lihavoinnin avulla, jotta haastateltavan vastauksien erottaminen helpottuu.

Minkälainen tiedon luokittelupolitiikka toisella yrityksellä oli (oliko monta eri tietoluokkaa)?

Yrityksen tiedoista suurin osa oli luokittelematonta tietoa. Tällä pyrittiin karsimaan luokittelun aiheuttamia kustannuksia. Varsinaisia tietoluokkia oli käytössä kolme:

- Private data
- Proprietary data
- Controlled/Restricted data

Salaisen tiedon säilytys (olivatko tiedot esim. pilvessä tai verkkolevyllä)?

Suurin osa yrityksen tiedoista säilytettiin verkkolevyillä ja osa oman koneen C-asemalla, jota ei kuitenkaan suositeltu säilytyspaikaksi. Tietoja oli myös SharePointissa, ja yhä enemmän tietoa pyrittiin tallettamaan mieluummin sinne kuin verkkolevyille tai koneelle. SharePointin ollessa vielä uusi palvelu yrityksessä monella ei tietotaito riittänyt sen käyttämiseen. Enemmän myös luotettiin vanhoihin säilytystapoihin, ja SharePointin turva-asetusten oikeaksi asettaminen koettiin liian vaikeaksi varsinkin vanhempien työntekijöiden mielestä. Tulostetut dokumentit tuli pääasiassa säilöä toimistolaatikostoon lukkojen taakse. SharePointissa oleviin tietoihin ohjeistettiin merkitsemään tiedon luokittelu, mutta kaikki eivät näin toimineet.

SharePoint antoi ilmoituksen, mikäli sivustolle yritettiin ladata luottamukselliseksi luokiteltua materiaalia ilman rajoituksien määrittämistä. Tiedoston lataaja sai siis heti ilmoituksen, jos dokumentin suojaukset eivät täyttäneet tarvittavia kriteereitä. Tämän vuoksi monet eivät merkinneet dokumentteja, koska eivät osanneet asettaa oikeita asetuksia SharePointiin.

Miten henkilöstöä ohjeistettiin ja kannustettiin tiedon luokitteluun?

Tiedon luokittelu kuului uuden työntekijän perehdytykseen, ja asiasta oli lisäksi käytävä vuosittain verkkokoulutus. Noin kuukausittain järjestettiin kontrollitarkastuksia, joissa tutkittiin tarkkaan kaikkien ehtojen täyttyminen. Tarkistettiin muun muassa oliko luottamuksellista aineistoa sisältävä laatikko lukossa vai ei. Työntekijöitä ei loppujen lopuksi niinkään kannustettu toimimaan oikein, vaan toiminta meni enemmän pakottamisen puolelle, ja säännöistä poikkeamisesta oli nollatoleranssi varsinkin fyysisten dokumenttien osalta.

Salattiinko kaikki salaiseksi luokiteltu tieto ja mitä suojaustoimenpiteitä salaiselle aineistolle tehtiin?

Salausta ei korostettu yhtä paljon kuin eri viitekohtien täyttymistä. Viitekohtia oli *Private*-tiedon kohdalla oltava vähintään kaksi. Tiedon oli oltava kahden lukon takana, joihin laskettiin lukittu ulko-ovi ja osaston tai työhuoneen lukittu ovi. Useimmiten pelattiin varman päälle ja käytettiin kolmen lukon menetelmää kahden sijaan. Tärkeimmillä tiedoilla oli oltava edellä olevien lisäksi vielä tietokoneen lukitus. Tässäkin tapauksessa oli yleensä neljä viitekohtaa käytössä, jotta kaikki ehdot varmasti täyttyisivät.

Controlled/restricted-tiedosta ei voida antaa kovinkaan varmaa vastausta, koska vain pienellä osalla henkilöstöstä oli hallussaan tällaista tietoa, mutta oletettavasti yritykselle erittäin luottamukselliseksi luokiteltu tieto salattiin. Salaus oli tarpeen varsinkin julkisissa tiloissa työskennellessä, sillä näissä tapauksissa tietokoneen lukitus oli riittämätön.

Luottamuksellista tietoa sisältävät paperit oli annettava henkilökohtaisesti vastaanottajalle. Mikäli tämä ei ollut paikalla, oli dokumentti laitettava *Private*-merkinnällä kirjekuoreen ja päälle oli kirjoitettava vastaanottajan nimi. Ainoastaan kyseinen henkilö sai avata kirjeen ja katsoa sen sisällön.

USB-muistitikkujen käyttö kiellettiin kokonaan. Lupa myönnettiin ainoastaan erikoistapauksissa, ja tällöin laite oli aina salattava ja säilytettävä huolellisesti.

Mitä mieltä olet nykyisen työnantajasi tiedon luokittelupolitiikasta?

Yrityksen tiedon luokittelupolitiikka on hyvin samantyyppinen toisen yrityksen kanssa, tosin hieman kevyempi. Yrityksellä on tärkeää olla kunnollinen luokittelupolitiikka, jonka luokkien määrittelyä tulisi verrata tietovuodosta aiheutuviin riskeihin. Toisen yrityksen SharePointissa oli enemmän mahdollisuuksia sivun omistajalla oikeuksien jakamisessa kuin kohdeyrityksellä. Omille sivuille pystyi luomaan sisältöä ja hallinnoimaan sen oikeuksia.

Kuinka luokittelu toteutettiin käytännössä? Olivatko kaikki sitoutuneita siihen?

Luokittelun toteutumista vahdittiin tarkkaan kuukausittaisten tarkastusten avulla. Jokaiseen tietoluokkaan kuuluvaan dokumenttiin ohjeistettiin merkitsemään sen tietoluokitus ja paperisille dokumenteille käytössä oli leimasimia tarkoitusta varten. Tästä huolimatta dokumenttien visuaalinen merkitseminen jäi vähemmälle. Enemmän luotettiin työntekijöiden osaamiseen tiedon luokituksen päättelemisessä ja oikeiden toimintatapojen noudattamisessa. Koulutus oli niin perusteellista, että henkilöstöllä voitiin katsoa olevan riittävät kyvyt tulkita kaikkien dokumenttien luokitus riippumatta siitä oliko siihen merkitty luokka vai ei.

Dokumentteja oli säilytettävä työntekijän arvion mukaisen luokan perusteella vaikka luokkaa ei olisi merkitty. Jos merkitseminen oli kunnossa, dokumenttia oli aina käsiteltävä merkityn luokan mukaan. Mikäli muistutuksia tuli, niitä saivat yleensä aina samat henkilöt. Pääasiassa kaikki panostivat tiedon luokitteluun omalta osaltaan. Muissa maissa saatetaan panostaa eri asioihin riippuen kyseisen maan tilanteesta, joten eri maiden osastoilla tiedon luokittelu ei välttämättä ole yhtä tärkeässä asemassa.

Oliko joku osasto tai henkilö vastuussa luokittelun ohjeistamisesta ja käytännön neuvonnasta?

Kaikkia pidettiin vastuullisina tiedon luokittelusta ja monet hoitivatkin sen omalta osaltaan. Paikallinen hallinto-osasto oli vastuussa henkilöstön koulutuksen järjestämisestä. Auditointia hoitavilla henkilöillä oli myös vastuu siitä, että säädöksiä noudatettiin.

6.2 Haastatteluanalyysi

Tiedon luokittelussa päätarkoituksena on löytää yrityksen tieto ja luokitella se sen arvon mukaisella tavalla. Toisella yrityksellä oli tähän käytössä kolme eri tietoluokkaa, joita olivat *Private Data*, *Proprietary Data* sekä *Controlled/Restricted Data*. Kohdeyrityksellä taas on käytössään *Internal*, *Restricted* ja *Secret* luokat. Luokkien nimitykset ovat erittäin selkeät ja näistä käy helposti ilmi minkä tyyppistä tietoa niiden alle kuuluu. Luokkia ei ole kummallakaan yrityksellä liian montaa, mikä helpottaa työntekijöiden työtä niiden tunnistamisessa. Tosin toisen yrityksen luokittelupolitiikka on jonkin verran tarkemmin määritelty kuin kohdeyrityksen politiikka, joka pitää sisällään myös julkisen tiedon, kun taas toisella yrityksellä luokiteltiin ainoastaan sellainen tieto, mikä vaati erityisiä suojatoimenpiteitä.

6.2.1 Tiedon luokittelupolitiikka yrityksissä

Toisessa yrityksessä kaikkea tietoa ei luokiteltu, vaan yrityksellä oli käytössään epäviralllinen tietoluokka, jossa olevia tietoja kutsuttiin luokittelemattomiksi tiedoiksi. Kyseiseen luokkaan kuului muun muassa kaikki julkinen tieto yrityksestä, kuten esimerkiksi intranetin uutiset, sekä sellainen tieto mikä ei kuulunut yhteenkään yrityksen kolmesta tietoluokasta. Päätös näiden tietojen luokittelematta jättämiseen oli kustannusselitteinen, sillä yrityksessä järjestettiin joka kuukausi kontrollitarkastuksia luokittelun suojatoimenpiteiden tarkistamiseksi. Kaiken tiedon luokittelun valvominen olisi tuottanut liian suuria kustannuksia sen tuottamaan hyötyyn nähden. Yrityksessä oli panostettu erittäin paljon työntekijöiden kouluttamiseen, joten henkilöstön voitiin olettaa tunnistavan eri tietoluokkiin kuuluvat tiedot ja osaavan käsitellä niitä luokittelupolitiikan vaatimalla tavalla.

Kohdeyrityksessä tiedon luokittelupolitiikkaa ollaan parhaillaan lanseeraamassa ja tarkoituksena on luokitella kaikki sähköisessä muodossa oleva tieto. Tieto tulisi luokitella

heti sen luomisvaiheessa, sillä dokumentin tekijä on todennäköisesti parhaiten tietoinen siitä, mitä suojatoimenpiteitä dokumentin käsittely vaatii ja näin ollen kykenee merkitsemään dokumentin oikealla tavalla. Toiseen yritykseen verrattuna tämän luokittelumenetelmän voidaan ajatella olevan hyödyllisempi ja selkeämpi käyttäjien kannalta varsinkin käytännön ollessa näin uusi. Kaikkien dokumenttien luokittelu auttaa henkilöstön sopeutumista ajatukseen tiedon luokittelusta. Toisaalta menetelmä saattaa tuottaa myös hankaluuksia luokittelun noudattamisen valvonnassa, sillä yleisen mielipiteen mukaan kaikkien sähköisten dokumenttien läpikäynti on erittäin aikaa vievää ja työlästä. Tarkoitukseen on kehitetty erilaisia ohjelmia, mutta niistä aiheutuvat ylimääräiset kulut saattavat paisua odottamattoman suuriksi.

6.2.2 Tiedon säilytys

Toisessa yrityksessä tietoja säilytettiin sekä verkkolevyillä että SharePointissa, jonne käyttäjiä kannustettiin tallettamaan suurin osa tiedoista. Tämä kuitenkin aiheutti ongelmia varsinkin vanhempien käyttäjien keskuudessa, sillä SharePointin luokituksien turva-asetusten asettaminen koettiin liian vaikeaksi ja näin ollen osa dokumenteista jätettiin luokittelematta. Kohdeyrityksen SharePointin käyttöönotto ei myöskään sujunut täysin ongelmitta, siitä huolimatta että yrityksellä koulutettiin muutamia Power Usereita, joiden tehtävänä oli kouluttaa omat osastolaisensa. Lopulta tästä käytännöstä luovuttiin, ja siirryttiin pitämään ajoittaisia SharePoint koulutuksia osastokohtaisesti. Suunnitelmissa on myös järjestää koko talolle avoimia koulutuksia, jotta SharePointin kaikkia ominaisuuksia päästään hyödyntämään. Luokittelussa ja sen toteutumisen auditoinnissa tulee olla tarkkana, että kaikki luokiteltavaksi tarkoitettu tieto käsitellään säännösten mukaan. Toisessa yrityksessä dokumenttien visuaalinen merkitseminen jäi taka-alalle, mikä johti siihen, että läheskään kaikkia dokumentteja ei merkitty. Tällaisessa tapauksessa saattaisi olla tarpeen painottaa tiedon merkitsemisen olevan osa tiedon luokittelua ja näin ollen siihen tulisi panostaa yhtä lailla kuin viitekohtiin.

Toisen yrityksen *Controlled/Restricted*-luokan dokumentit todennäköisesti salattiin aina ennen niiden tallettamista. Kyseisiä dokumentteja oli ainoastaan pienellä osalla henkilöstöä, joten enimmäkseen korostettiin eri viitekohtien täyttymistä, joihin laskettiin erityyppiset lukot aina ulko-oven lukosta tietokoneen lukitukseen. Näiden seikkojen täyttymistä valvottiin kuukausittaisilla tarkastuksilla sekä vuosittain suoritettavalla verkkokou-

lutuksella. Tiedon luokitteluun suhtauduttiin toisella yrityksellä vakavasti ja tiedon luokittelematta jättäneiden toimiin puututtiin hanakasti. Ottamalla tiukan linjan luokittelun suhteen saatiin lähes koko henkilöstö hoitamaan oman osuutensa ja tiedostamaan vastuunsa asian suhteen. Tosin luokittelun ja viitekohtien tärkeyden painottaminen meni melkeinpä pakottamisen puolelle. Jatkuvat kontrollit viitekohtien tarkastamiseen johtivat siihen että niitä noudatettiin pilkun tarkkaan, mutta itse dokumenttien merkitseminen jäi vähemmälle. Työntekijät luottivat omiin ja työtovereidensa taitoihin tunnistaa mihin tietoluokkaan mikäkin dokumentti kuuluu.

6.2.3 Tiedon luokittelun implementointi

Kohdeyrityksellä pyritään ottamaan tiedon luokittelupolitiikka osaksi henkilöstön työrutiinia, tarkoituksena tehdä luokittelusta lähes automaattinen prosessi, jonka käyttäjä suorittaa jo heti dokumentin luomisvaiheessa. Toisin kuin toisella yrityksellä ei kohdeyrityksellä korosteta fyysistä tietosuojaa salaisen tiedon käsittelyssä niin paljon kuin salauksen merkitystä. Salaisten dokumenttien ympäristön tai vaihtoehtoisesti itse dokumenttien on oltava salattuja, jotta tieto voidaan tallettaa säännösten mukaisesti. Kohdeyrityksellä tullaan ottamaan käyttöön Secure SharePointiksi kutsuttu salattu ympäristö helpottamaan käyttäjien tiedonhallintaa kun taas toisella yrityksellä käytettiin tiedostojen salausmenetelmää. Tiedon suojaukseen liittyvissä asioissa on tarpeen tehdä asiat käyttäjille mahdollisimman yksikertaisiksi, jotta he muistavat panostaa omalta osaltaan tiedon turvaamiseen. Säädösten ollessa helposti noudatettavissa käyttäjälle ei tule sellaista oloa ettei kykene osallistumaan tiedon suojaamiseen siksi, että menetelmät olisivat liian monimutkaisia tai aikaa vieviä.

6.3 Tiedon luokittelupolitiikan merkitys käyttäjälle

Tämän analysoinnin materiaaleina hyödynnän yrityksen käyttöön tulevaa *IT Community Regulation* -dokumenttia, maailmalla käytettäviä yleisiä luokittelukäytäntöjä, kohdeyrityksen salaisen tiedon käsittelyyn olevaa ohjeistusta sekä aiemmin toisella yrityksellä työskennelleen henkilön haastattelua. Haastattelussa verrattiin henkilön nykyisen yrityksen luokittelupolitiikkaa hänen entisellä työnantajallaan olleeseen luokitteluun. Haastateltava

ei haastattelun aikana toiminut aikaisemman yrityksen edustajana, ja haastattelussa esitetyt mielipiteet ja näkökulmat olivat hänen omiaan. Kyseiseen yritykseen viitataan tässä tekstissä nimityksellä ”yritys X”.

6.3.1 Tiedon luokittelun visuaalinen merkitseminen

Tiedon luokittelussa päätarkoituksena on löytää yrityksen tieto ja luokitella se sen arvon mukaisella tavalla. ISO 27001 -standardissa määritellään yleiset tiedon luokittelun menetelmät, joita voidaan soveltaa yrityksen käyttöön. Kohdeyrityksessä standardin neljästä luokasta on sovellettu käyttöön kolme, jotka ovat *Internal, Restricted* ja *Secret.* Määritelmät ovat riittävän kattavat ja selkeät, mahdollistaen tiedon luokittelun jo dokumentin luomisvaiheessa yrityksellä käytössä olevalla Labeling Toolilla. Kyseisen Microsoft Office -työkalun avulla voidaan luokitella Word- ja PowerPoint-dokumentteja, mikä helpottaa käyttäjien työtä tiedon visuaalisessa merkitsemisessä. Siitä huolimatta että yrityksellä suositellaan luokiteltavaksi kaikki uusi tieto, on ongelmia ilmennyt jo ennen säädösten varsinaista implementointia. Yrityksellä on salaista tietoa mainittujen tiedostomuotojen lisäksi myös Excel-tiedostoina aiheuttaen ongelmia visuaalisen merkitsemisen suhteen, sillä työkalua ei ole mahdollista hyödyntää Excelissä.

Visuaalisen merkitsemisen ollessa puutteellista korostuu koulutuksen ja tiedon eteenpäin välittämisen tarve. Tiedon lähettäjälle ja vastaanottajalle jää vastuu siitä, että Excel-tiedostoja käsitellään niiden vaatimien luokitusten mukaisesti, sillä merkinnän puuttuessa on tiedon käsittelijän pääteltävä luokitus itse ja kohdeltava dokumenttia vaadituin toimenpitein. Yritys X:llä oli käytössään menetelmä, jossa luokiteltiin ainoastaan oikeuksiltaan rajattu tieto, joten esimerkiksi intranetuutisia ei luokiteltu lainkaan. Kyseisessä yrityksessä korostettiin luokittelun merkitystä, ja koulutuksia järjestettiin tasaisin väliajoin. Näin voitiin varmistaa, että henkilöstöllä oli tarvittavat taidot tiedon luokituksen tunnistamiseen merkitsemisen puutteellisuudesta huolimatta. Tosin vastuun jättäminen tiedon käsittelijöille tuo aina mukanaan omat riskinsä, joita tulisi pyrkiä vähentämään mahdollisuuksien mukaan.

6.3.2 Salaisen tiedon säilytyspaikat ja -tavat

Salaisen ja luottamuksellisen tiedon säilytyspaikkojen ja -tapojen olisi oltava mahdollisimman käyttäjäystävällisiä, jotta tiedon säilyttämisessä vaaditut ehdot täyttyisivät. Kummassakin tarkasteltavassa yrityksessä tietojen säilytykseen käytettiin verkkolevyjä ja SharePointia. SharePointin käyttöönotossa oli molemmilla yrityksillä hieman ongelmia koulutuksien järjestämisestä huolimatta. Yritys X:llä ongelmia ilmeni eniten vanhemmilla käyttäjillä, jotka eivät osanneet asettaa SharePointin asetuksia vastaamaan tiedon luokittelua. Voidaan kuitenkin olettaa yritys X:n luottamuksellisten tietojen olleen salattuja toisin kuin kohdeyrityksessä, jossa kaikki salainen tieto ei ollut salatussa ympäristössä tai muutoin salattuna. Parhaillaan implementoitavana olevassa luokittelupolitiikassa korostetaan salauksen merkitystä tiedon suojauksessa, ja tätä menetelmää tullaan jatkossa vaatimaan joko tiedon säilytyspaikalta tai tiedostolta itseltään. Yritykseen tullaan hankkimaan Secure SharePointiksi kutsuttu salattu ympäristö salaisen tiedon säilytystä varten. Kyseinen säilytyspaikka muistuttaa ulkonäöltään tavallista SharePoint-sivustoa, joten sen käytettävyys on selkeää henkilöille, jotka käyttävät aktiivisesti tavallistakin SharePointia. Käyttäjän ei myöskään tarvitse huolehtia yksittäisten tiedostojen salauksesta, sillä ympäristö salaa tiedostot automaattisesti helpottaen erittäin paljon työskentelyä.

Tiedostojen salausta saatetaan kuitenkin tarvita joissain tapauksissa, joten tarkoitusta varten yrityksellä on käytössään Microsoft Office -dokumenttien salaus. Muut dokumentit voi salata 7-Zip-ohjelman avulla, mikä tosin vaatii hieman enemmän toimenpiteitä käyttäjältä. Yhtenä huonona ominaisuutena 7-Zipissä voidaan pitää sitä, että salatun kansion sisällä olevien tiedostojen nimet pääsee näkemään. Vaikka tiedostoja ei saa auki ilman salasanaa, aiheuttaa jo pelkkä kansion sisällön näkeminen matala-asteisen tietoturvahaitan. Tiedostojen salauksessa korostuu salasanan turvallisen tallettamisen tärkeys. Salatut tiedostot voi avata ainoastaan salasanan avulla, joten tämän unohtuessa tai kadotessa ei käyttäjällä ole enää mitään mahdollisuutta saada tiedostoa auki, eivätkä edes IT-tukihenkilöt voi auttaa tässä tilanteessa. Tämä on huomioitu ja yritys tarjoaa KeePass-ohjelmaa, jonne voi tallettaa salasanansa turvallisesti. Kyseiset seikat huomioon ottaen, päätös ottaa käyttöön Secure SharePoint helpottaa käyttäjien asemaa ja vähentää heihin kohdistuvia paineita.

Yksittäisen säilytyspaikan määrittämisellä vältetään tiedon vuotaminen ja saman tiedon sijaitseminen useassa eri paikassa. Lisäksi korostamalla yhden säilytyspaikan merkitystä voidaan ehkäistä tiedon väärään paikkaan tallettamista. Monet tiedon käsittelijät

tallettavat salaisiksi luokiteltuja tietoja omalle työpöydälleen, tietokoneen C-asemalle tai sähköpostiinsa. Kyseiset säilytyspaikat ovat kuitenkin uuden politiikan mukaan kiellettyjä. Mikäli salaista tietoa on lähetettävä sähköpostitse, on sen aina oltava salatussa muodossa. Microsoft Outlookin avulla sähköpostin salaaminen on mahdollista, tosin ulkoiselle kumppanille viestiä lähetettäessä on tehtävä ensimmäisellä kerralla allekirjoitusten hyväksyntä, jotta salattujen viestien lähettäminen onnistuu.

Ennen salaisten tiedostojen välittämistä on aina kysyttävä lupa tiedon omistajalta. Ilman omistajan hyväksyntää tiedostoja ei saa lähettää eteenpäin, muokata tai poistaa. On myös huolehdittava, ettei tiedon luokitus häviä tai muutu ilman painavaa syytä. Näihin seikkoihin on kiinnitetty huomiota yrityksen luokittelupolitiikassa ja tästä syystä visuaalisen merkitsemisen tärkeyttä korostetaan, sillä sen avulla tiedon vastaanottaja kykenee käsittelemään tietoa sen vaatimalla tavalla eikä luokitteluvirheitä näin ollen pitäisi syntyä.

6.3.3 Johtopäätökset

Uuden luokittelupolitiikan käyttöönotto on tärkeä askel tietoturvan parantamisessa ja tiedon suojaamisessa. Tietovuotojen sekä -murtojen yleistymisen huomioon ottaen yrityksen tiedon turvaaminen on yksi avainasioista, jotka on otettava huomioon työrutiineissa. Tästä syystä yrityksiin tarvitaan vahva tiedon luokittelupolitiikka, jonka avulla pyritään minimoimaan mahdolliset tietovuodot ja helpottamaan tiedon hallinnointia. Nämä seikat huomioon ottaen yritykselle on onnistuttu luomaan vankka politiikka, joka auttaa työntekijöitä suojaamaan käsittelemänsä tiedon ja antaa ohjeistusta oikeiden toimenpiteiden noudattamiseen. Käyttäjän työpanos on pyritty pitämään mahdollisimman pienenä ja helposti noudatettavana, mikä laskee huomattavasti tiedon luokitteluun ryhtymisen kynnystä.

6.4 Henkilöstökoulutus

Yrityksen salaisen tiedon käsittelyn ohjeistus on koottu konsernin tarjoamien ohjeiden ja säädösten pohjalta. Ohjeisiin keräsin yrityksen tarjoamat menetelmät tiedon salaukseen ja luokitteluun. Näihin kuului sähköpostiviestien (Liite 1 ja 2) ja Microsoft Office-dokumenttien (Liite 3) salaus sekä 7-zip ohjelman (Liite 4) ja Windowsin BitLockerin (Liite 5) käyttö salauksessa. Lisäksi yritys tarjoaa Labeling Tool -nimistä (Liite 6) työkalua Word-

ja PowerPoint-dokumenttien merkitsemiseen, minkä käytöstä ja siihen liittyvistä ongelmista kokosin oman ohjeistuksen yrityksen intranetissä tarjolla olevien materiaalien perusteella.

Ohjeiden valmistuttua kokosin henkilöstökoulutukseen tarvittavat materiaalit. Salaisen tiedon säilytystä varten tilattiin Secure SharePoint -niminen ympäristö, jonka esittely oli osana koulutusta. Koulutuksia salaisen tiedon säilytyksestä ja käsittelystä pidettiin yhteensä kolme kappaletta: kaksi Turussa ja yksi Espoossa. Koulutuksen pitäjänä toimin enimmäkseen itse projektivastaavan avustuksella. Koulutuksessa kerrattiin ensin hieman eri tietoluokituksia, ja kerrottiin kuinka salaista tietoa tulee käsitellä sen elinkaaren eri vaiheiden aikana.

Yritykselle käyttöön tulevaa Labeling Toolia esiteltiin dian verran, kuten myös eri salaustapoja. Näissä käytin hyväkseni aiemmin suomentamiani ohjeita, tiivistäen dioihin ydinasiat eri menetelmistä. Secure SharePointin ominaisuuksia ja käyttötarkoituksia käsiteltiin muutaman dian verran ja kyseinen ympäristö saikin aikaan jonkin verran keskustelua ja kysymyksiä. Koulutuksen tarkoituksena oli rohkaista käyttäjiä Secure SharePointin käyttöönotossa, ja tarjota heille mahdollisuus antaa parannusehdotuksia ulkoasun suhteen. Olikin siksi positiivista huomata yleisön olleen kiinnostuneita Secure SharePointista ja sen käyttämisestä.

Pilvipalveluiden hyödyntämisestä on käyty paljon keskustelua myös kohdeyrityksessä, joten pilven hyötyihin ja haittoihin paneuduttiin myös muutaman dian verran. Konsernilla on tarjolla ohjeet pilvipalveluiden käyttöönottoprosessiin, joten kyseisiä ohjeita käsiteltiin muutamalla sanalla ja rohkaistiin käyttäjiä tutustumaan niihin. Esitykseen oli koottu muutamat yrityksen kannalta tärkeät huomioon otettavat seikat. Nämä ja pilvipalveluiden käytön mahdollisuudet herättivät paljon keskustelua ja tästä heränneitä kysymyksiä pohdittiin osallistujien kesken.

Esityksen lopuksi esiteltiin Secure SharePointia ja sen ominaisuuksia. Osallistujia ohjeistettiin valitsemaan jokaiselle osastolle oma vastuuhenkilö, josta tulee osaston tietojen omistaja. Kyseiselle henkilölle on tarkoitus antaa vastuu käyttäjien lisäämisestä eri kirjastoihin. Näin omistajat voivat itse hallinnoida oikeuksien antamista ja poistamista, eikä prosessin tarvitse kulkea IT-osaston kautta. Tarkoituksena on vähentää IT:n osallistumisen tarvetta, sillä omistajat itse ovat todennäköisesti parhaiten tietoisia siitä keillä on tarvetta päästä tietoihin käsiksi.

Tarkoituksena on laittaa suomennetut ohjeet yrityksen intranetiin koko henkilöstön nähtäville helpottamaan käyttäjien tiedon luokittelun aikana mahdollisesti ilmenevien ongelmien selvittämisessä. Palaute koulutuksista oli erittäin positiivista, ja koulutuksia tullaan tarvittaessa pitämään lisää. Koulutusmateriaalista on myös englanninkielinen versio. Materiaali lisättiin yrityksen intranetiin ja oheen liitettiin linkit alkuperäisiin ohjeisiin ja sivustoihin.

7 YHTEENVETO

Tiedon luokittelun eri luokkien ja menetelmien implementoiminen yritykselle oli aloitettu jo viime vuoden puolella, joten salaisen tiedon luokitteluun perehtyminen, ohjeiden suomentaminen ja koulutuksien pitäminen osui oikeaan saumaan käyttäjien kannalta. Projektilla on ollut tiukka aikataulu, ja opinnäytetyössä käsitellyt ja tehdyt työt auttoivat projektin eteenpäin saattamisessa huomattavasti.

Projektin alussa tutustuin jo tehtyyn pohjatyöhön tiedon luokittelusta ja keräsin tietoa yritykselle tehdyistä vaatimuksista ja ohjeistuksista. Huomasin nopeasti, että tiedonlähteenä toimiva sivusto oli erittäin epäselkeästi rakennettu ja osa tärkeistä tiedoista oli ripoteltu sivuston reunoilla sijaitseviin linkkeihin tai piilotettu erikseen auki klikattavien osien alle. Todettiin, että suomenkielisten ohjeiden tekeminen tulisi tarpeeseen, ja koottuani kaikki tarpeelliset tiedot tein ohjeet salaisen tiedon käsittelystä ja siihen käytettävistä menetelmistä.

Salaisen tiedon käsittelystä pidettiin koulutuksia henkilöille, jotka ovat paljon tekemisissä salaisen tiedon kanssa. Koulutusten tavoitteena oli kannustaa osallistujia ottamaan käyttöön Secure SharePoint -nimisen ympäristön, jonka tarkoituksena on helpottaa käyttäjien työtä salaisen tiedon säilyttämisessä ja käsittelyssä. Lisäksi koulutuksessa kerrattiin salaisen tiedon käsittelyn eri vaiheita, eri salausmenetelmiä ja käsiteltiin muutamalla dialla pilvipalveluita. Suomentamani ohjeet ja koulutuksessa käyttämäni materiaali lisätään yrityksen intraan, minne tulee myös englanninkielinen versio koulutusmateriaalista. Koulutuksia tullaan pitämään lisää tarvittaessa.

Voidaan todeta tavoitteiden täyttyneen odotusten mukaisesti ja työn valmistuneen aikataulussa. Henkilöstölle on koottu mahdollisimman helppokäyttöiset ohjeet tiedon oikeaoppiseen luokitteluun yrityksen standardien mukaan. Salaisen tiedon säilytyspaikka saatiin hankittua, ja sen käyttöönotto on parhaillaan työn alla. Teoriaosuudessa käsitellyt asiat tiedon ja salaisen tiedon luokittelusta pohjustivat erittäin hyvin projektin alkuun saattamista ja avarsivat kirjoittajan näkemystä tiedon luokittelusta. Projektin aikana toteutettu haastattelu antoi perspektiiviä yritykselle luotavien ohjeistuksien ja koulutuksien suunnittelussa.

LÄHTEET

Barker, W.; Fahlsing, J.; Gulick, J. 2008. Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories. Viitattu 2.2.2016 http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf.

Bradley, T. 2016. Pros and Cons of Bringing Your Own Device to Work. Viitattu 2.3.2016 http://www.pcworld.com/article/246760/pros_and_cons_of_byod_bring_your_own_device_.html.

Cisco. 2008. How Virtual Private Networks Work. Viitattu 15.4.2016 http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html

Crawford, D. 2014. 5 most secure backup services. Viitattu 14.3.2016 https://www.bestvpn.com/blog/10907/5-most-secure-backup-services/.

Crawford D. 2015. SpiderOak Or Wuala: Which is More Secure? Viitattu 10.3.2016 http://www.cloudwards.net/spideroak-or-wuala-which-is-more-secure/.

EMC Corporation. 2006. EMC Infoscape user Quide. Viitattu 16.3.2016 ftp://ftp.legato.com/pub/legato/manufacturing/V4%20Binaries/InfoScape/emcinfoscape1_0_ug.pdf.

EMC Education Services. 2012. Information Storage and Management. Indianapolis: John Wiley & Sons.

ENISA. 2009. Cloud Computing: Benefits, risks and recommendations for Information Security. Viitattu 4.3.2016 https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

Etges, R. & McNeil, K. 2006. Understanding Data Classification Based on Business and Security Requirements. Viitattu 3.2.2016 http://www.isaca.org/Journal/archives/2006/Volume-5/Documents/jopdf0605-understanding-data.pdf.

Fowler, S. 2003. Information Classification. Who, Why and How. Viitattu 3.2.2016 https://www.sans.org/reading-room/whitepapers/auditing/information-classification-who-846.

Hakala, M.; Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo.

Huotari, M-J. 2016. Viitattu 27.1.2016 http://oppimateriaalit.internetix.fi/fi/avoimet/0viestinta/informaatiotutkimus/po1/perusteet/01_mita_tieto_on/.

IEC. 2016. Viitattu 22.3.2016 http://www.iec.ch/.

Information Classification Policy. Viitattu 2.2.2016 http://www.iso27001security.com/ISO27k_Model_policy_on_information_classification.pdf.

ISO. 2016. Viitattu 22.3.2016 http://www.iso.org/iso/home.html.

Järvinen, P. 2006. Paranna Tietoturvaasi. Jyväskylä: Docendo.

Microsoft. 2016a. BitLocker Drive Encryption Overview. Viitattu 8.4.2016 http://windows.microsoft.com/en-us/windows-vista/bitlocker-drive-encryption-overview.

Microsoft. 2016b. What is Lync Basic? Viitattu 8.4.2016 https://support.office.com/en-us/article/What-is-Lync-Basic-a1821c3d-7631-483c-8791-3d16b10b844d?ui=en-US&rs=en-US&ad=US

Mohamed, A. 2008. Data classification: why it is important and how to do it. Viitattu 3.2.2016 http://www.computerweekly.com/feature/Data-classification-why-it-is-important-and-how-to-do-it.

National Institute of Standards and Technology. 2016. NIST Cloud Computing Program. Viitattu 10.3.2016 http://www.nist.gov/itl/cloud/index.cfm.

Simberkoff, D. 2016. The Challenges of Data Classification. Viitattu 3.2.2016 http://www.net-security.org/article.php?id=2298&p=1.

Smallwood, R. & Blair, B. 2012. Safeguarding Critical E-Documents: Implementing a Program for Securing Confidential Information Assets. New Jersey: John Wiley & Sons.

The Free Dictionary By Farlex. 2016. CWID. Viitattu 8.4.2016 http://acronyms.thefreedictionary.com/CWID

Xerox Corporation. 2016. Smarter Document Management. Viitattu 16.3.2016 http://www.xrce.xerox.com/Customer-Led-Innovation/Themes/Next-Generation-Managed-Print-Services/Smarter-Document-Management.

Withee K. 2013. SharePoint 2013 For Dummies. New Jersey: John Wiley & Son.

Woody, A. 2013. Enterprise Security: A Data-Centric Approach to Securing the Enterprise. Birmingham: Packt Publishing Ltd.

Kryptattujen sähköpostien lähettäminen ulkoiselle kumppanille

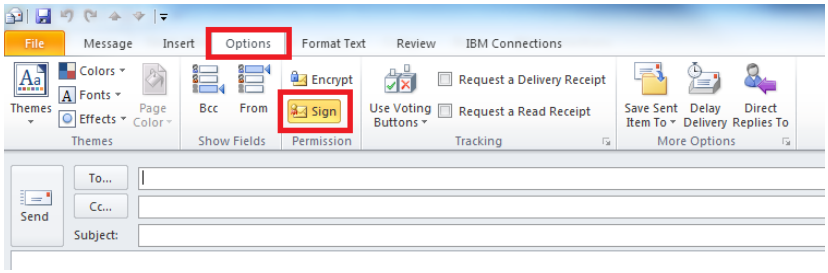
Luottamuksellisten tietojen lähettäminen sähköpostitse vaatii sähköpostin kryptaamista, jotta asiattomat henkilöt eivät pääse lukemaan tai muokkaamaan sähköpostin sisältöä. Tarve korostuu erityisesti ulkoisten yhteistyökumppanien kanssa kommunikoidessa.

Ulkoisilla kumppaneilla on oltava kryptausvaihtoehtona S/MINE. Mikäli tämä vaihtoehto ei ole käytettävissä, kryptattujen sähköpostien välittäminen ei onnistu.

Sertifikaatin lähetys ja yhteystiedon tallentaminen

Ennen kuin kryptatun viestin voi lähettää, on ensimmäiselle kerralla vaihdettava sertifikaatti tai avain vastaanottajan kanssa.

Ensin on lähetettävä allekirjoitettu sähköposti ulkoiselle kumppanille. Tämä onnistuu Outlookista avaamalla ***New E-mail*** ja kirjoittamalla vastaanottajan osoitteen. Mene ***Options***-välilehdelle ja etsi ***Permission***-osiosta ***Sign***-kohta. Klikkaa se aktiiviseksi ja lähetä sähköposti. Pyydä kontaktiasi ilmoittamaan onnistuiko sähköpostin lähetys ja pyydä häntä lähettämään vastaavanlainen ***external***-sertifikaatti.



Kaikki kontaktin lähettämät sertifikaatit on tunnistettava turvallisiksi kryptattujen viestien lähettämisen mahdollistamiseksi. Avaa viesti ja klikkaa lähettäjän osoitteen oikeassa laidassa olevaa kuvaketta.

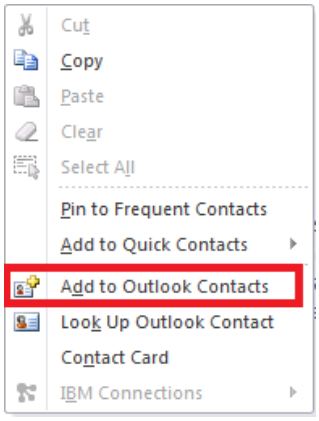
Digital Signature Invalid -ikkunan auetessa klikkaa ***Trust***.

Sähköpostista ja käyttöjärjestelmästä riippuen ikkunat saattavat olla erinäköisiä kumppanisi ruudulla. Ongelmatilanteissa vastaanottajan on syytä ottaa yhteyttä omaan IT-tukeen.

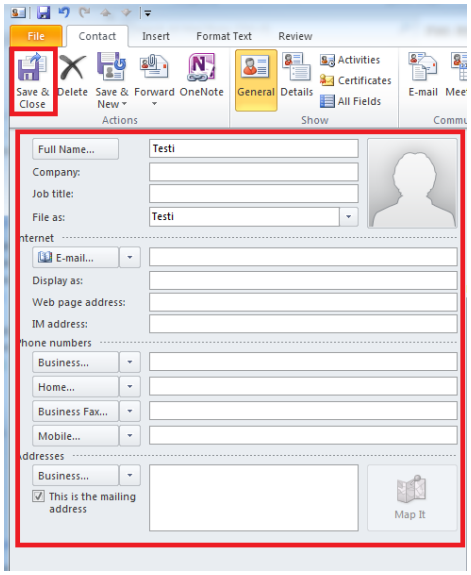
Ulkoisen kumppanin on hyväksyttävä varoitusikkunan ilmoittamat toimet klikkaamalla ***Yes***-kohtaa**.** Seuraavaksi lähettäjän sertifikaatit asentuvat.

Ulkoisen kumppanin tallennettua lähettämäsi sertifikaatin, lähettää tämä allekirjoitetun sähköpostin, joka on avattava ja hyväksyttävä samaan tapaan kuin aiemmin kuvatussa.

Sähköpostin saatuasi tallenna kontakti Outlookin osoitekirjaan klikkaamalla oikealla hiiren painikkeella kontaktisi sähköpostiosoitetta ja valitsemalla ***Add to Outlook Contacts***.

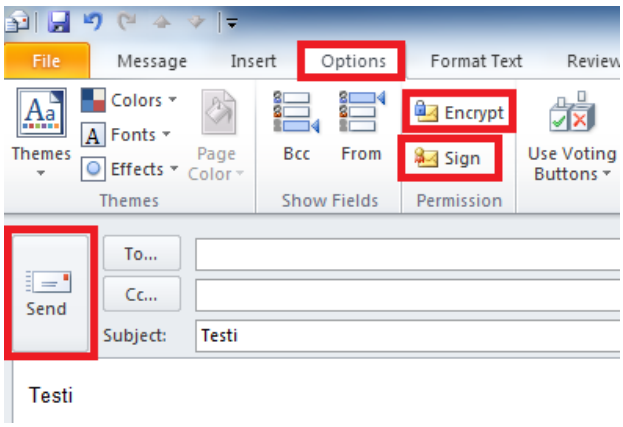


Kirjaa tarvittavat tiedot ylös ja paina yläkulmasta ***Save and Close***. Tämä toimenpide tallentaa automaattisesti ulkoisen kumppanin sertifikaatin yhdessä kontaktitietojen kanssa.



Kryptattujen sähköpostien lähettäminen

Lähettääksesi kryptatun sähköpostiviestin ulkoiselle kumppanille, avaa uusi sähköposti ja lisää vastaanottaja. ***Options***-välilehdeltä ***Permission***-kohdasta löytyvät ***Encrypt***- ja ***Sign***-kohdat**.** Klikkaa kyseiset kohdat aktiivisiksi ja lähetä sähköpostiviesti.



Kontaktisi vastaanottaa kryptatun viestisi ja voi lähettää takaisin kryptattuja vastauksia tai kokonaan uusia kryptattuja viestejä. Kryptatut viestit tunnistaa lukon mallisesta ikonista.

Kryptattujen sähköpostiviestien lähettäminen

Sähköpostiviestin kryptaaminen Microsoft Outlookilla muuttaa tavallisen tekstin kryptattuun muotoon. Kyseisen tavan mahdollistamiseksi lähettäjän ja vastaanottajan on vaihdettava vastaavanlaiset avaimet, jotta vastaanottaja kykenee lukemaan viestin.

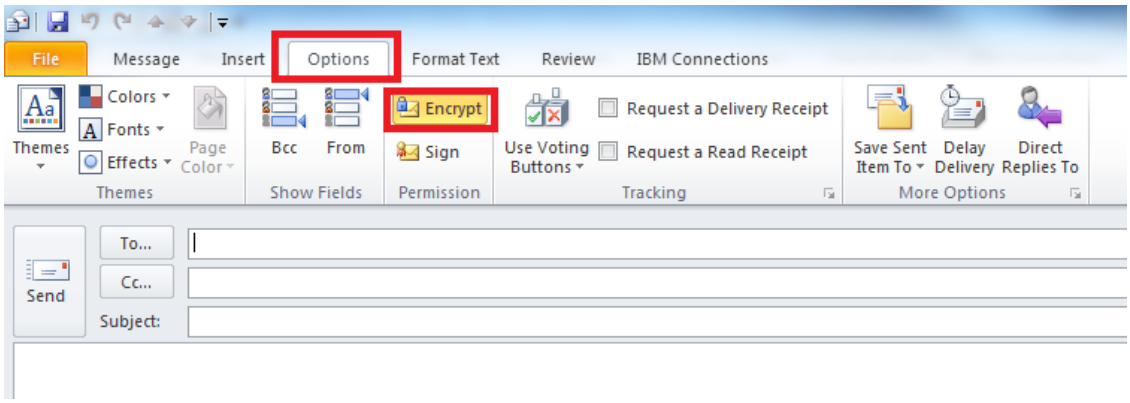
Yrityksellä sisäiset avaimet vaihtuvat automaattisesti Outlook-käyttäjien välillä.

Mikäli lähetät kryptatun viestin henkilölle, jonka sähköposti ei tue kryptausta, saat ilmoituksen Outlookilta. Jos haluat lähettää viestin joka tapauksessa, on sinun ensin poistettava siitä kriittiset tiedot ja lähetettävä ne kryptattuna liitetiedostona.

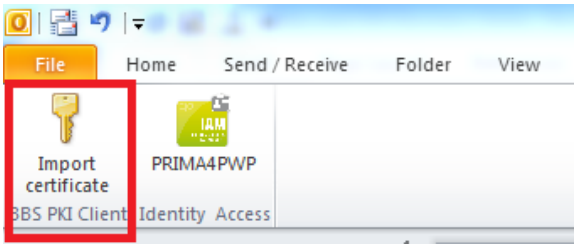
Kryptattu sähköpostiviesti kryptaa myös kaikki siinä olevat liitetiedostot. Nämä ovat kuitenkin kryptattuja ainoastaan sähköpostissa. Koneelle ladatessa kryptaus ei enää toimi, joten tiedostot on syytä tallettaa turvalliseen ympäristöön.

Viestin kryptaaminen

Avaa uusi viesti ja mene ***Options***-välilehdelle. ***Permission-***osiosta löytyy ***Encrypt***-kohta**,** joka on klikattava aktiiviseksi.



Jos sinulla ei näy yllä olevaa näkymää, on sinun ensin aktivoitava se menemällä ***"Yrityksen nimi"***-välilehdelle Outlookissa ja klikkaamalla ***PKI Client*** -ryhmässä ***Import certificate***-kohtaa.

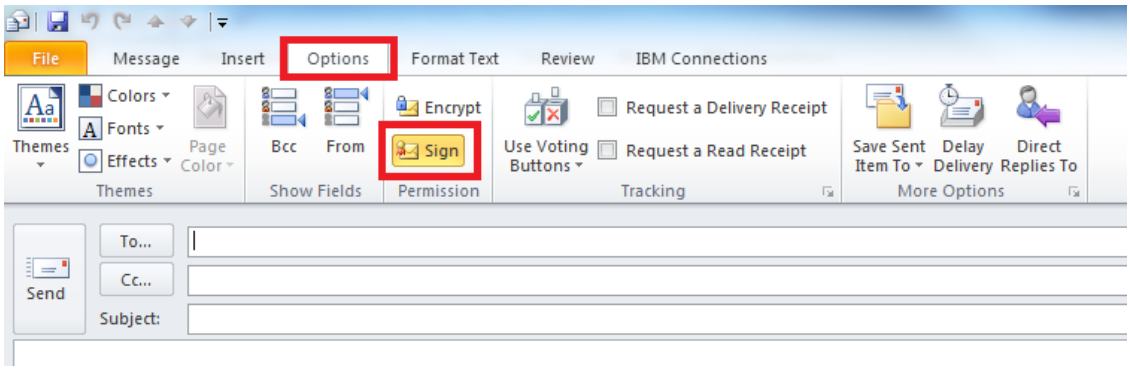


Tarkistaaksesi kryptauksen, avaa ***sent items*** -kansio ja tarkista viestin esikatselusta tai itse viestistä näkyykö siinä kumpaakaan lukkoikonia.

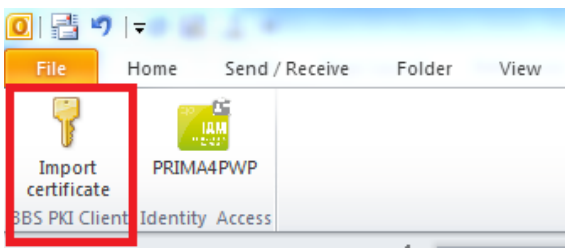
Mikäli ikoni näkyy, on viesti lähetetty kryptatussa muodossa.

Viestin allekirjoittaminen

Avaa uusi viesti ja mene ***Options***-välilehdelle. ***Permission***-osiosta löytyy ***Sign***-kohta**,** joka on klikattava aktiiviseksi.



Jos sinulla ei näy yllä olevaa näkymää, on sinun ensin aktivoitava se menemällä ***"Yrityksen nimi"***-välilehdelle Outlookissa ja klikkaamalla ***PKI Client*** -ryhmässä ***Import certificate***-kohtaa.



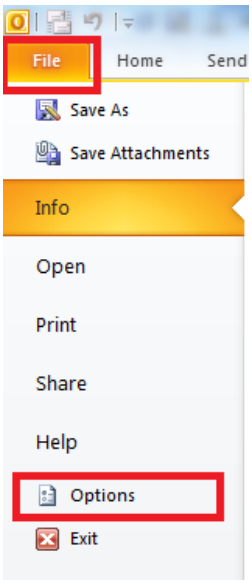
Tarkistaaksesi allekirjoituksen, avaa ***sent items*** -kansio ja tarkista viestin esikatselusta tai itse viestistä näkyykö siinä kumpaakaan allekirjoitusikoneista. 

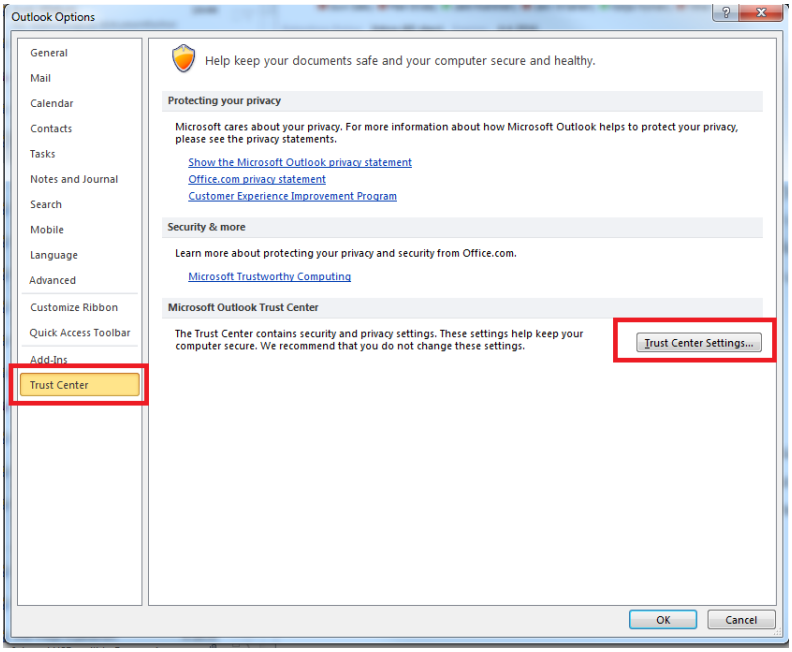
Mikäli ikoni näkyy, on viesti lähetetty allekirjoitettuna.

Kaikkien lähetettävien sähköpostien kryptaaminen tai allekirjoittaminen

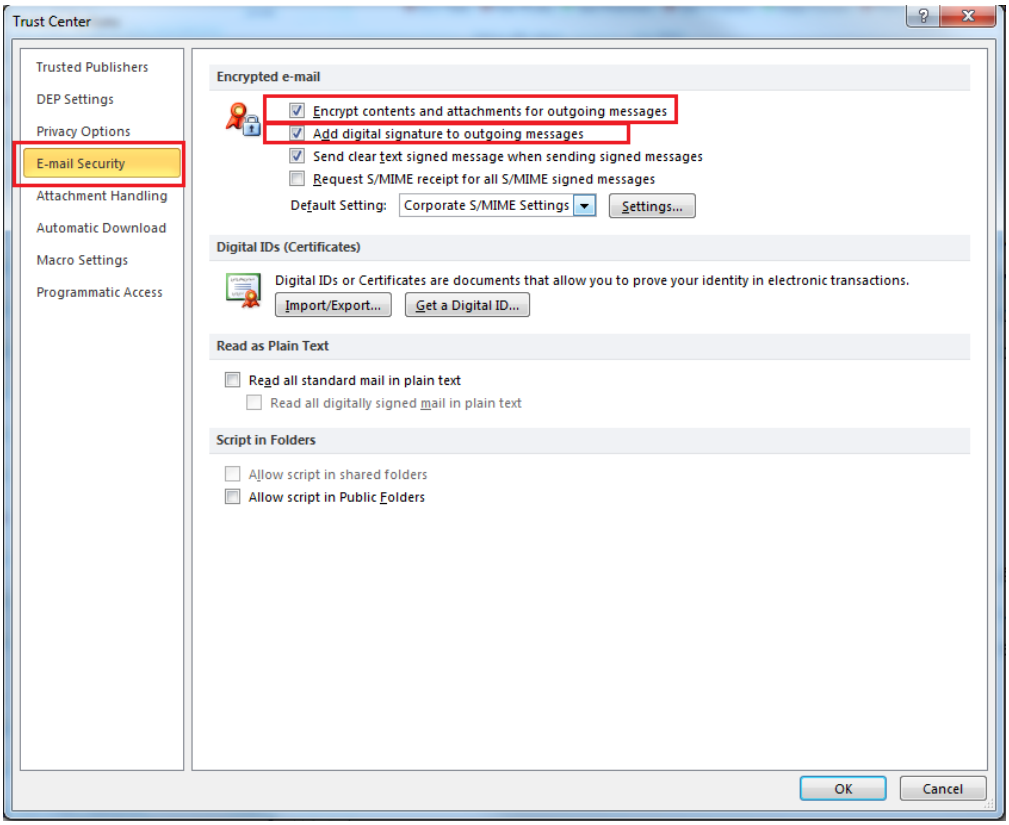
Jos haluat oletuksena lähettää kaikki viestisi kryptattuina tai allekirjoitettuina, vastaanottajalla on myös oltava kryptaus aktivoituna viestien katsomisen mahdollistamiseksi. Kryptauksen saa aktivoitua ***”Yrityksen nimi”***-välilehdeltä.

Automaattisen kryptauksen mahdollistamiseksi, mene ***File***-välilehdelle ja klikkaa auki ***Options***-kohta**.** Mene ***Trust Center*** -välilehden kautta ***Trust Center Settings*** -kohtaan.





Email Security -kohdassa laita ruksi ***Ecrypt contents and attachments for outgoing messages*** -kohtaan**,** mikäli haluat automaattisen kryptauksen päälle. Allekirjoituksen saa aktivoitua laittamalla ruksin ***Add digital signature to outgoing messages*** -kohtaan.



Sulje Trust Center ja Outlookin asetukset klikkaamalla ***OK*** molemmissa ikkunoissa.

Microsoft Office-dokumentin kryptaaminen

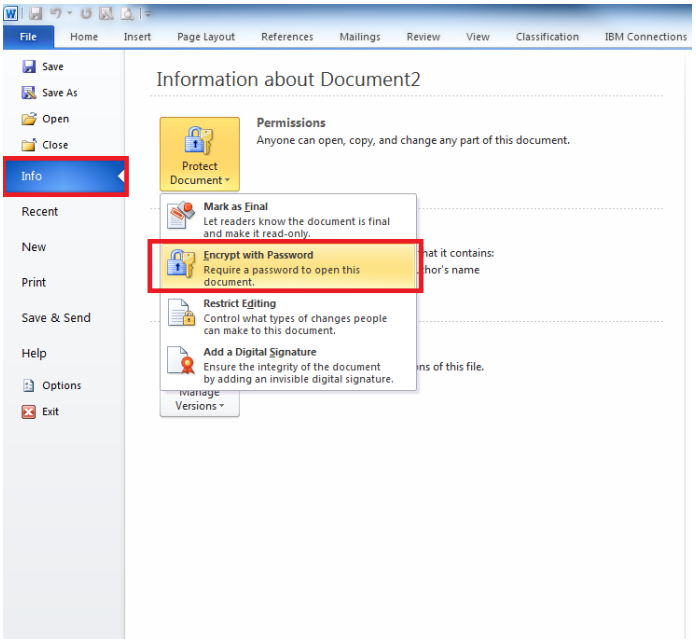
Kaikki muualla kuin Secure SharePointissa sijaitsevat dokumentit on kryptattava MS Officen kryptauksen avulla turvallisen säilytyksen varmistamiseksi.

Mikäli tiedoston kryptauksessa käytetty salasana unohtuu, sitä ei kykene avaamaan edes Service Desk tai administraattori!

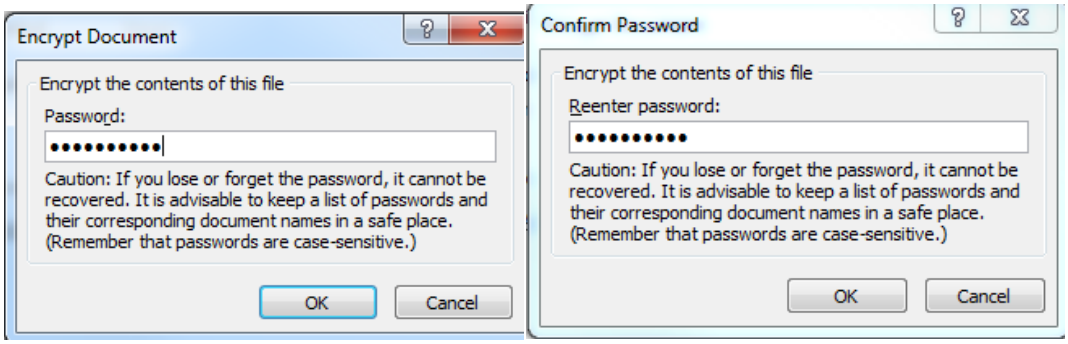
Jos tiedostoa muokkaa useampi kuin yksi henkilö, on salasana talletettava KeePassiin. Huomioi seuraavat kohdat:

- Dokumentti on kryptattava vahvalla salasanalla.
- Kaikki dokumentin käsittelijät käyttävät samaa salasanaa.
- KeePassia käytetään dokumentin salasanan turvalliseen tallettamiseen.
- Auktorisoiduille käyttäjille ilmoitetaan salasana erikseen (esimerkiksi puhelimitse).
- Eri salasanoja tulee käyttää eri projekteissa.
- Jos salasana päätyy valtuuttamattomien henkilöiden tietoon, on se vaihdettava viipymättä, ja kyseisen salasanan omaavat tiedostot on kryptattava uudella salasanalla.

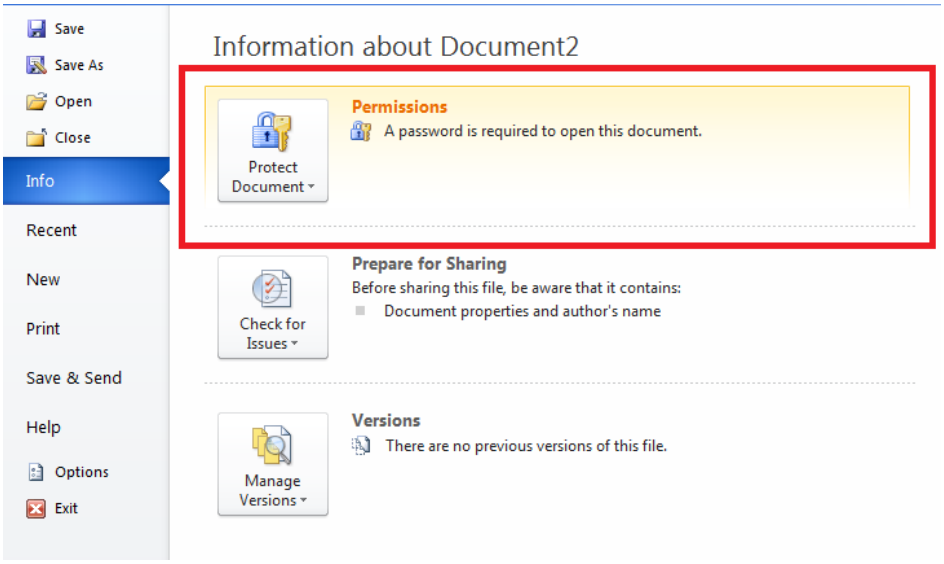
Aloittaaksesi dokumentin kryptauksen avaa tiedosto, jonka haluat kryptata ja mene ***File***-välilehdellä ***Info***-kohtaan. Oikealla on ***Protect Document*** -kohta, jota klikkaamalla aukeaa pudotusvalikko. Valitse ***Encrypt with Password***.



Encypt Document -ikkunan auettua näppäile haluamasi salasana ja paina ***OK***. Tämän jälkeen aukeaa ***Confirm Password*** -ikkuna, joka pyytää salasanan kirjoittamista uudelleen. Salasanan kirjoitettuasi, paina ***OK***.



Onnistuneen kryptauksen jälkeen dokumentin ***Info***-osiossa pitäisi näkyä seuraavanlainen ilmoitus:



Valitessasi salasanaa käytä vähintään kahdeksaa merkkiä sisältäen sekä suuria että pieniä kirjaimia (A-Z, a-z), numeroita (0,1, …, 9) ja jos mahdollista niin myös erikoismerkkejä (~!@#$%^&*_-+=´|\(){}[]:;”<>,.?/). Älä kuitenkaan käytä salasanassasi kirjaimia ä, ö tai å.

Varmista että salasanassasi on vähintään kolme edellä mainituista vaihtoehdoista. Salasana ei saisi sisältää nimiä (etu/sukunimi, toinen nimi, tyttönimi ym.) tai CWID-tunnusta.

Vältä sanakirjasta löydettävien termien käyttöä, tiettyjä merkkijonoja tai yhdistelmiä (rivejä näppäimistöstä, kuten ”...asdf…” tai ”…4567…” tai ”…aaa…”). Älä myöskään käytä termejä, jotka viittaavat itseesi tai ympäristöösi (yrityksen nimi, osasto tai projekti, sukulainen, lemmikki ym.).

Tiedoston kryptaus 7-zipillä

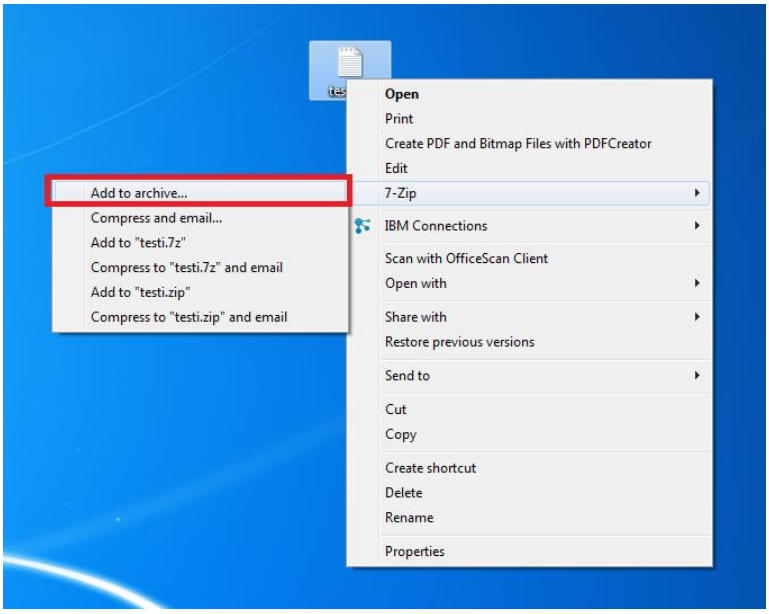
Kaikki muualla kuin Secure SharePointissa sijaitsevat dokumentit on kryptattava 7-zipin avulla turvallisen säilytyksen varmistamiseksi. Tämä kryptausmenetelmä on tarkoitettu pääasiassa muille kuin Microsoft Office tiedostoille. MS Office tiedostoille on erikseen omat ohjeensa.

Mikäli tiedoston kryptauksessa käytetty salasana unohtuu, sitä ei kykene avaamaan edes Service Desk tai administraattori!

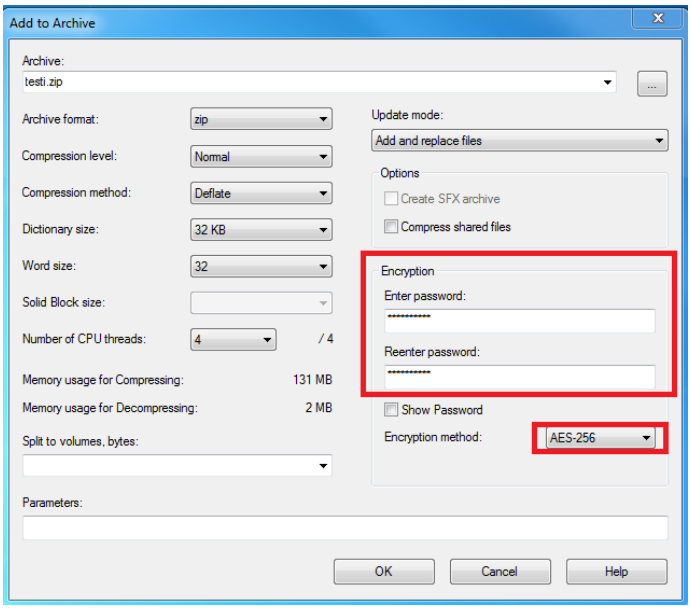
Jos tiedostoa muokkaa useampi kuin yksi henkilö, on salasana talletettava KeePassiin. Huomioi seuraavat kohdat:

- Dokumentti on kryptattava vahvalla salasanalla.
- Kaikki dokumentin käsittelijät käyttävät samaa salasanaa.
- KeePassia käytetään dokumentin salasanan turvalliseen tallettamiseen.
- Auktorisoiduille käyttäjille ilmoitetaan salasana erikseen (esimerkiksi puhelimitse).
- Eri salasanoja tulee käyttää eri projekteissa.
- Jos salasana päätyy valtuuttamattomien henkilöiden tietoon, on se vaihdettava viipymättä, ja kyseisen salasanan omaavat tiedostot on kryptattava uudella salasanalla.

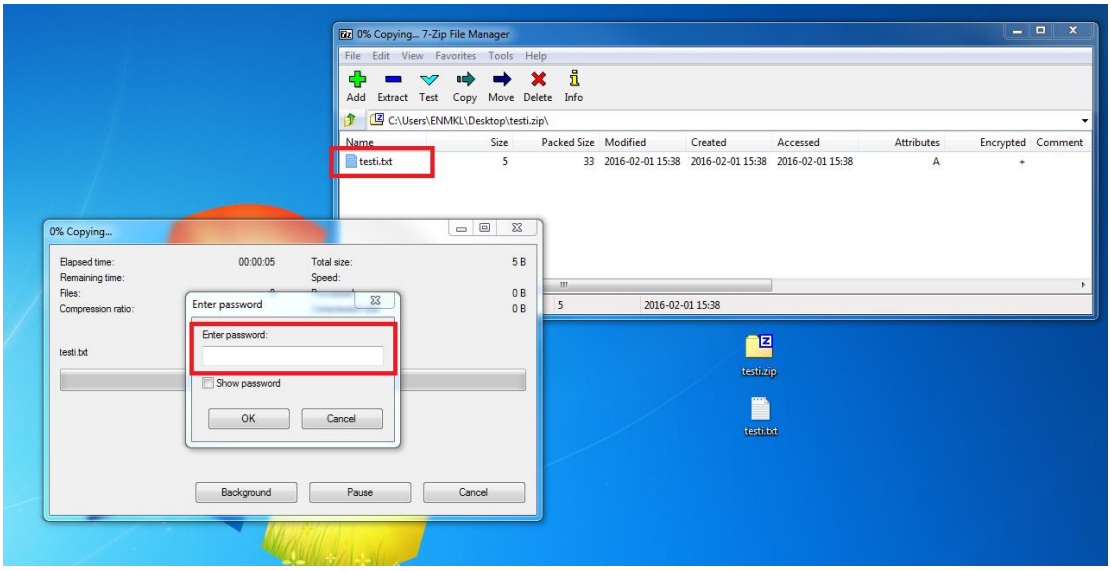
Aloittaaksesi tiedoston kryptaamisen 7-zipillä, on dokumentti ensin lisättävä 7-zip ***File Manageriin*** klikkaamalla hiiren oikeaa painiketta ja valitsemalla 7-zipin kohdalta ***Add to archive***.



Add to Archive -ikkunan auettua kirjoita haluamasi salasana ***Enter Password*** ja ***Reenter password*** -kenttiin ja vaihda ***Encryption methodin*** kohdalle ***AES-256***. Paina ***OK*** painiketta.



Mikäli olet jättänyt muut oletusasetukset paikalleen, kryptatun tiedoston pitäisi olla tallennettuna samaan kansioon. Avaa arkisto tuplaklikkaamalla kansiota ja arkiston auettua tuplaklikkaa kryptattua tiedostoa. Tämän jälkeen sinua pyydetään kirjoittamaan luomasi salasana, minkä jälkeen tiedosto aukeaa.



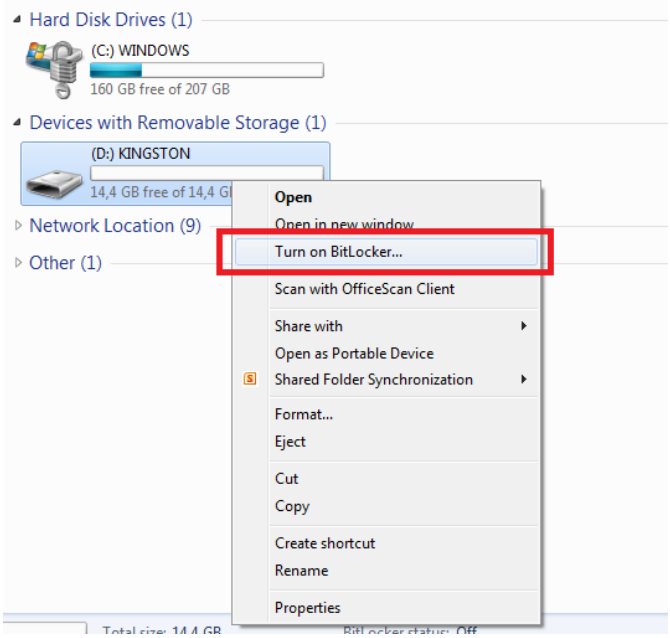
Valitessasi salasanaa käytä vähintään kahdeksaa merkkiä sisältäen sekä suuria että pieniä kirjaimia (A-Z, a-z), numeroita (0,1, …, 9) ja jos mahdollista niin myös erikoismerkkejä (~!@#$%^&*_-+=´|\(){}[]:;”<>,.?/). Älä kuitenkaan käytä salasanassasi kirjaimia ä, ö tai å.

Varmista että salasanassasi on vähintään kolme edellä mainituista vaihtoehdoista. Salasana ei saisi sisältää nimiä (etu/sukunimi, toinen nimi, tyttönimi ym.) tai CWID-tunnusta.

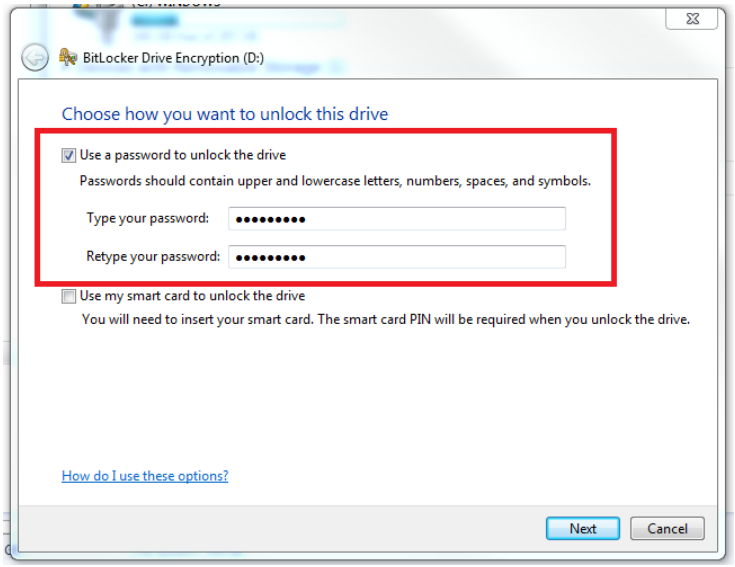
Vältä sanakirjasta löydettävien termien käyttöä, tiettyjä merkkijonoja tai yhdistelmiä (rivejä näppäimistöstä, kuten ”...asdf…” tai ”…4567…” tai ”…aaa…”). Älä myöskään käytä termejä, jotka viittaavat itseesi tai ympäristöösi (yrityksen nimi, osasto tai projekti, sukulaisia, lemmikkejä ym.).

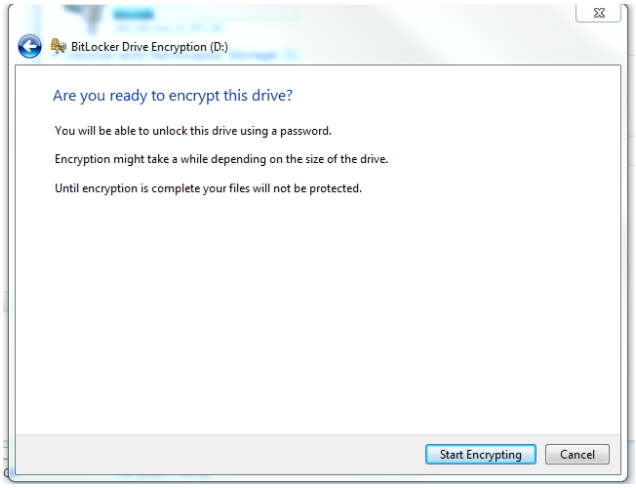
USB-tikun kryptaaminen BitLockerilla

USB-tikun kryptaamalla voi pienellä vaivalla estää ulkopuolisten henkilöiden pääsyn laitteen tiedostoihin. Aloittaaksesi kryptauksen laita ensin tikku kiinni koneeseen, minkä jälkeen mene ***Start***-valikkoon ja valitse oikealta kohta ***Computer*.** Tikkusi pitäisi näkyä ***Devices with Removable Storage*** -kohdan alla. Klikkaa USB-laitetta oikealla hiiren painikkeella ja etsi kohta ***Turn on BitLocker…***



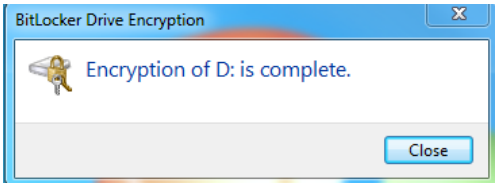
Laita ruksi ***Use a password to unlock the drive*** -kohtaan ja kirjoita haluamasi salasana. Klikkaa ***next***.





Paina ***Start Encrypting,*** ja BitLocker aloittaa laitteen kryptaamisen. Voit käyttää konettasi normaalisti, kunhan et poista laitetta koneesta ennen kryptauksen valmistumista. Laitteen koosta riippuen kryptaamisessa saattaa kestää useita minuutteja. Jos laite on saatava irti koneesta ennen kuin kryptaus on valmis, paina **pause** ja irrota tämän jälkeen tikku turvallisesti koneesta.

Kryptauksen valmistuttua voit sulkea ikkunan painamalla ***Close.***



Laittaessasi laitteen uudelleen kiinni koneeseen BitLocker kysyy asettamaasi salasanaa. Kirjoita salasana ja paina ***Unlock***.

Labeling Tool

Labeling Tool -merkitsemistyökalun tehtävänä on helpottaa Word- ja PowerPoint-tiedostojen luokittelua. Merkitsemisen tarkoituksena on osoittaa visuaalisin keinoin, mitä turvatoimenpiteitä kyseisen dokumentin käsittely vaatii. Tässä tulisi noudattaa seuraavia ohjeita:

- **Internal**
  - Tieto on julkista kaikille yrityksen työntekijöille. Ulkoistetuille toimijoille tietoa pyritään jakamaan vain tarvittaessa.
- **Restricted**
  - Ainoastaan rajatulla määrällä ryhmiä on oikeus nähdä ja käsitellä tietoa. Tiedon omistajan määrittelemän ryhmän lisäksi tietoa saa jakaa muille ainoastaan tarpeen niin vaatiessa.
- **Secret**
  - Erittäin tärkeää tietoa, joten tiedon tarkasteluun ja käsittelyyn tarvittavia oikeuksia rajoitetaan. Tiedon omistaja määrittää oikeudet ja myöntää luvat tiedon eteenpäin luovuttamiselle. Salainen tieto on aina kryptattava ja säilytettävä turvallisessa ympäristössä.

Jokainen uusi dokumentti on merkittävä merkitsemistyökalulla yllä olevat seikat huomioon ottaen. Merkintä ilmaantuu dokumentin oikeaan alalaitaan alatunnisteen kohdalle. Työkalu on optimoitu yrityksen asiakirjapohjien mukaan, joten uusia dokumentteja tehdessä tulisi pyrkiä käyttämään kyseisiä pohjia.

Merkitsemistyökalua voidaan tällä hetkellä käyttää ainoastaan Word- ja PowerPoint-dokumenttien merkitsemiseen, joten PDF-dokumenttien merkitseminen ei ole mahdollista. Word- tai PowerPoint-dokumentin voi merkitsemisen jälkeen muuttaa PDF-muotoon, jossa merkintä on näkyvissä. Makrot saattavat myös aiheuttaa ongelmia Labeling Tool -työkalun käytössä. Tällöin kyseinen dokumentti on ensin tallennettava omalle koneelle Word-tiedostona (*.docx), minkä jälkeen sen voi luokitella. On muistettava, että luokittelu ei kryptaa dokumenttia vaan toimii ainoastaan leimana dokumentin alareunassa dokumentin tunnistamisen helpottamiseksi.

Luokittelutyökalun löytää Word- ja PowerPoint-tiedoston ***Classification-***välilehdeltä. Klikkaamalla ***IS Classification*** -kuvaketta saat eri tietoluokitukset näkyviin. Valitse oikea

luokitus klikkaamalla sitä, minkä jälkeen se ilmestyy dokumentin alatunnisteeseen. Kun haluat poistaa tai muokata luokitusta, valitse ***Classification***-välilehdeltä ***Remove All Labels*** -kohta**,** minkä jälkeen voit halutessasi valita uuden luokituksen.

Dokumentin asetuksiin tehdyt muutokset saattavat joskus vaikuttaa siihen ettei merkintä näy kunnolla dokumentin alareunassa. Asetuksien muutoksilla tarkoitetaan tässä tapauksessa sivun formatointia, ulkoasua tai alatunnistetta. Ongelman saa korjattua ***Classification***-välilehdellä valitsemalla ***Remove all labels***.

Mikäli käytät muita kuin yrityksen omia asiakirjapohjia, näissä ei ole välttämättä lainkaan alatunnistetta, joten sellainen on luotava ”Insert”-välilehdeltä kohdasta ”Footer”. Tämän pudotusvalikosta valitaan ”Edit Footer”. Lisäksi osa valmiiden pohjien ala- ja ylätunnisteista saattaa aiheuttaa ongelmia merkitsemistoiminnon kanssa.

Virheilmoitus ”Error in (first) page footer placement” saattaa merkitä sitä, että tiedostossa on kappaleen vaihto, joka estää merkitsemisen. Menemällä ”Home”-välilehdelle ja aktivoimalla sieltä formatointimerkinnät saadaan näkyviin kohta ”section break (next page)” sivun alalaidasta. Tämä on korvattava tavallisella sivunvaihdolla.

Pidettäessä esityksiä yrityksen ulkopuolella, ei merkintöjä käytetä. Restricted ja Secret materiaalia ei ole lupa esittää ulkopuolisille, minkä vuoksi merkintöjä ei tässä tapauksessa tarvita. Myöskään yrityksen sisäisesti suuremmalle yleisölle pidettävässä esityksessä ei saa esittää muuta kuin Internal-tunnuksella luokiteltua materiaalia. Kaikille ulkopuolisille toimijoille pidettäville esityksille on hankittava lupa yrityksen viestintäosastolta. Yrityksen ulkopuolisille lähetettävässä tiedossa luokittelu on tarpeen, mikäli ulkopuolisen toimijan ja yrityksen välisessä sopimuksessa niin lukee.